UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Magistrsko delo

Predstavitev naravnih števil kot vsote kvadratov

(Representing positive integers as sum of squares)

Ime in priimek: *Tjaša Košenina*
Študijski program: *Matematične znanosti, 2. stopnja*
Mentor: *prof. dr. Štefko Miklavič*

Koper, oktober 2022

Ključna dokumentacijska informacija

Ime in PRIIMEK: Tjaša KOŠENINA

Naslov magistrskega dela: Predstavitev naravnih števil kot vsote kvadratov

Kraj: Koper

Leto: 2022

Število listov: 67 Število referenc: 6

Mentor: prof. dr. Štefko Miklavič

UDK: 511.3(043.2)

Ključne besede: teorija števil, predstavitev naravnih števil kot vsote kvadratov, konguence, Legendrovi simboli, Gaussova lema, Jacobijevi simboli, Gaussov zakon kvadratne recipročnosti, kvadratni ostanek in neostanek, mali Fermatov izrek, Willsonov izrek, Princip golobnjaka, Thueva lema, Fermatov izrek, kvadratna forma v treh spremenljivkah, Eulerjeva funkcija, Eulerjev kriterij, Dirichletov izrek o aritmetičnem zaporedju, Eulerjeva lema, Lagrangev izrek

Math. Subj. Class. (2020):

Izvleček:
Glavna tema magistrskega dela so rezultati glede predstavitve naravnih števil kot vsote kvadratov. Najprej so v poglavju *Pomožne definicije in izreki* navedene splošne definicije in izreki, katere potrebujemo v nadaljevanju. Sledi poglavje v katerem predstavimo katera naravna števila lahko zapišemo kot vsoto dveh kvadratov. Nato sledi poglavje s predstavitvijo naravnih števil, katere lahko zapišemo kot vsoto treh kvadrato. Na koncu je še poglavje v katerem dokažemo, da lahko vsako naravno število predstavimo kot vsoto štirih kvadratov. Sledi poglavje, v katerem predstavimo na koliko načinov lahko naravno število zapišemo kot vsoto štirih kvadratov. V zaključku so predstavljena nadaljna vprašanja, ki se nam lahko porodijo na podlagi predstavljene vsebine.

Key document information

Name and SURNAME: Tjaša KOŠENINA

Title of the thesis: Representing positive integers as sum of squares

Place: Koper

Year: 2022

Number of pages: 67 Number of references: 6

Mentor: Prof. Štefko Miklavič, PhD

UDC: 511.3(043.2)
Keywords: number theory, representing positive integer as sum of squares, congruence, Legender symbol, Gauss's lemma, Jacobi symbol, Gauss quadratic reciprocity theorem, quadratic residue and nonresidue, Fermat's little theorem, Willson's theorem, Pigeonhole principle, Thue's lemma, Fermat's theorem, definite ternary forms, Euler function, Euler's criterion, Dirichlet's theorem on arithmetic progressios, Euler's lemma, Lagrange theorem

Math. Subj. Class. (2020):

Abstract:
The main topic of the master's thesis are results regarding the representation of positive integers as sums of squares. The first chapter contains some general definitions and theorems that we used later. In the second chapter we presents result regarding positive integers, that can be written as a sum of two squares. Then follows the chapter with the presentation of positive interegs, which can be written as a sum of three squared. At the end, there is a chapter in which we prove that every positive integer can be represented as a sum of four squares. The last chapter presents in how many ways a natural number can be written as a sum of four squares. In the conclusion, further questions that may arise based on the presented content are presented.

Kazalo vsebine

Zahvala

Zahvaljujem se mentorju prof. dr. Štefko Miklaviču za vso pomoč, hitro odzivnost, razumevanje, razlago in za vse nasvete pri pisanju magistrskega dela.
Zahvaljujem se svojim staršem, fantu Maticu, prijateljicama Ivani in Neji za vso spodbudo pri pisanju svoje naloge.

1 UVOD

Katero je najmanjše naravno število n, da lahko vsako naravno število zapišemo kot vsoto največ n kvadratov? To je vprašanje s področja teorije števil, ki je v preteklosti pritegnilo pozornost kar nekaj matematikov.
Za prvih nekaj naravnih števil velja

$$1 = 1^2,$$

$$2 = 1^2 + 1^2,$$

$$3 = 1^2 + 1^2 + 1^2,$$

$$4 = 2^2,$$

$$5 = 2^2 + 1^2,$$

$$6 = 2^2 + 1^2 + 1^2,$$

$$7 = 2^2 + 1^2 + 1^2 + 1^2,$$

$$\vdots$$

Torej je odgovor na zgornje vprašanje $n \geq 4$.

Nekatera števila lahko zapišemo kot vsoto samo dveh kvadratov in sicer Fermat je dokazal, da lahko liho praštevilo p zapišemo kot vsoto dveh kvadratov, če in samo če je $p \equiv 1 \ (mod \ 4)$ (primer $13 = 3^2 + 2^2$). Kasneje so dokazali, da je ta zapis enoličen. Dokazali so tudi, da če je p praštevilo oblike $4k + 3$ se ga zagotovo ne da zapisati kot vsoto dveh kvadratov. Ampak, če v razcepu naravnega števila na prafaktorje nastopajo praštevila oblike $4k + 3$ ter so ta na sode potence, potem lahko število zapišemo kot vsoto dveh kvadratov (primer $153 = 3^2 \cdot 17 = 12^2 + 3^2$). Zanimivo je tudi dejstvo, kako iz števil, ki jih lahko zapišemo kot vsoto dveh kvadratov, dobimo novo število, ki ga prav tako lahko zapišemo kot vsoto dveh kvadratov. In sicer, če imamo dve števili, ki jih lahko zapišemo kot vsoto dveh kvadratov, potem lahko tudi njun produkt zapišemo kot vsoto dveh kvadratov [1].

Skoraj vsa števila lahko zapišemo kot vsoto treh kvadratov, izjeme so števila oblike $4^n(8m + 7)$, kjer sta m in n nenegativni celi števili. Formalen dokaz tega je v začetku 19. stoletja objavil Legendre. V dokazu je uporabil znanje s področja kongruenc,

kvadratnih form v treh spremenljivkah, Legendrovih simbolov, Jacobijevih simbolov, Lagrangev izrek ter Dirichletov izrek o aritmetičnih zaporednjih. S problemom, katera števila lahko zapišemo kot vsoto treh kvadratov, so se pred njim ukvarjali tudi drugi matematiki. Fermat je ugotovil, da lahko števila oblike 3m+1 zapišemo kot vsoto treh kvadratov, vendar tega ni dokazal. Njegovo idejo je potem uporabil Beguelin ter dokazal, da vsa števila oblike 8n+7 ne moremo zapisati kot vsoto treh kvadratov [3].

Končni odgovor na začetno vprašanje pa je $n = 4$. To dejstvo je dokazal matematik Lagrange leta 1772, ko je objavil dokaz izreka, da lahko vsako naravno število zapišemo kot vsoto štirih kvadratov, pri čemer so nekateri kvadrati lahko enaki 0. V dokazu je uporabil že nekatera prej dokazana dejstva, recimo, da lahko vsako praštevilo zapišemo kot vsoto štirih kvadratov, ter Eulerjev izrek, da če sta m in n števili, ki ju lahko zapišemo kot vsoto štirih kvadratov, potem lahko tudi število mn zapišemo kot vsoto štirih kvadratov [1].

2 POMOŽNE DEFINICIJE IN IZREKI

Oglejmo si nekaj pomožnih definicij in izrekov, katere bomo uporabili v nadaljevanju. Najprej definirajmo pojem kongruenca in nekaj njenih lastnosti ter vpeljimo njeno oznako. Ta koncept je prvi vpeljal nemški matematik Karl Friedrich Gauss v svojem delu Disquisitiones Arithmeticae, katerega je objavil pri svojih rosnih 24 letih. Zanj je bilo področje teorije števil eno najpomembnejših področij matematike. Rekel je "Matematika je kraljica znanosti in teorija števil je kraljica matematike." Začetni del, ki govori o kongruencah je povzet po [1].

Definicija 2.1. Naj bo n pozitivno število. Celi števili a in b sta kongruentni po modulu n, zapisano s simbolom

$$a \equiv b \pmod{n},$$

če n deli razliko $a - b$. To pomeni, da je $a - b = kn$ za neko celo število k.

Izrek 2.2. *Za poljubni celi števili a in b velja, da je $a \equiv b \pmod{n}$, če in samo če dasta a in b enak nenegativen ostanek pri deljenju z n.*

Dokaz. ($\Rightarrow$) Recimo, da velja $a \equiv b \pmod{n}$, torej je $a = b + kn$ za neko celo število k. Če število b delimo z n, ga lahko po izreku o deljenju zapišemo kot $b = qn + r$, kjer je $0 \leq r < n$ ter q celo število. Potem za a velja

$$a = b + kn = (qn + r) + kn = (q + k)n + r,$$

kar pomeni, da imata a in b res enak ostanek r pri deljenju z n.
($\Leftarrow$) Poglejmo še dokaz v drugo smer. Recimo, da data a in b enak ostanek pri deljenju z n, torej jih lahko zapišemo kot $a = qn + r$ ter $b = pn + r$, kjer sta q in p celi števili ter $0 \leq r < n$. Potem velja

$$a - b = (qn + r) - (pn + r) = (q - p)n,$$

torej n deli $a - b$. V jeziku kongruenc to pomeni, da je $a \equiv b \pmod{n}$. □

Izrek 2.3. *Naj bo n fiksno naravno število in a, b, c, d poljubna cela števila. Potem veljajo naslednje lastnosti:*

1. $a \equiv a \pmod{n}$.

2. *Če je* $a \equiv b \pmod{n}$, *potem je* $b \equiv a \pmod{n}$.

3. *Če je* $a \equiv b \pmod{n}$ *in* $b \equiv c \pmod{n}$, *potem je* $a \equiv c \pmod{n}$.

4. *Če je* $a \equiv b \pmod{n}$ *in* $c \equiv d \pmod{n}$, *potem je* $a + c \equiv b + d \pmod{n}$ *in* $ac \equiv bd \pmod{n}$.

5. *Če je* $a \equiv b \pmod{n}$, *potem je* $a + c \equiv b + c \pmod{n}$ *in* $ac \equiv bc \pmod{n}$.

6. *Če je* $a \equiv b \pmod{n}$, *potem je* $a^k \equiv b^k \pmod{n}$ *za vsako naravno število* k.

Dokaz. 1.: Za vsako celo število a velja, da je $a - a = 0 \cdot k$, torej je $a \equiv a \pmod{n}$.

2.: Če je $a \equiv b \pmod{n}$, potem je $a - b = nk$ za neko celo število k. Iz tega sledi, da je $b - a = -(nk) = (-k)n$. Ker je $-k$ prav tako celo število, sledi, da je $b \equiv a \pmod{n}$.

3.: Če je $a \equiv b \pmod{n}$ in $b \equiv c \pmod{n}$, potem velja, da je $a - b = hn$ in $b - c = kn$, za neki celi števili h in k. Iz tega sledi

$$a - c = (a - b) + (b - c) = hn + kn = (h + k)n.$$

Ker je $h + k$ celo število, velja da je $a \equiv c \pmod{n}$.

4.: Če je $a \equiv b \pmod{n}$ in $c \equiv d \pmod{n}$, potem velja $a - b = hn$ in $c - d = kn$ za neki celi števili h in k. Iz tega sledi

$$(a + c) - (b + d) = (a - b) + (c - d) = hn + kn = (h + k)n,$$

torej je $a + c \equiv b + d \pmod{n}$, saj je $h + k$ celo število. Prav tako velja tudi, da je

$$ac = (b + hn)(d + kn) = bd + bkn + dhn + hkn^2$$

$$ac - bd = (bk + dh + hkn)n.$$

Ker je $bk + dh + hkn$ celo število, sledi da je $ac \equiv bd \pmod{n}$.

5.: Sledi neposredno iz točke 4., saj je $c \equiv c \pmod{n}$.

6.: To točko bomo dokazali z indukcijo. Trditev očitno velja za $k = 1$. Torej predpostavimo, da trditev velja za nek k. Torej vemo, da je $a \equiv b \pmod{n}$ in $a^k \equiv b^k \pmod{n}$. Zaradi točke 4. sledi $aa^k \equiv bb^k \pmod{n}$, kar je ekvivalentno $a^{k+1} \equiv b^{k+1} \pmod{n}$. Torej trditev velja tudi za $k + 1$. S tem je točka 6. dokazana. □

Izrek 2.4. *Če je* $ca \equiv cb \pmod{n}$, *potem je* $a \equiv b \pmod{\frac{n}{d}}$, *kjer je* $d = gcd(c, n)$.

Dokaz. Če je $ca \equiv cb \pmod{n}$, potem velja

$$c(a-b) = ca - cb = kn \tag{2.1}$$

za neko celo število k. Ker je $d = gcd(c, n)$, potem obstajata tuji števili r in s, da velja $c = dr$ in $n = ds$. Če to vstavimo v (2.1) dobimo

$$r(a-b) = ks.$$

Iz tega sledi, da $s|r(a-b)$, ampak ker sta r in s tuji števili, velja da $s|a-b$, kar pomeni, da je $a \equiv b \pmod{s}$, to pomeni, da je $a \equiv b \pmod{\frac{n}{d}}$, saj je $s = \frac{n}{d}$. □

Posledica 2.5. *Če je* $ca \equiv cb \pmod{n}$ *in* $gcd(c, n) = 1$, *potem je* $a \equiv b \pmod{n}$.

Poseben primer Posledice 2.5 je naslednja posledica.

Posledica 2.6. *Če je* $ca \equiv cb \pmod{p}$ *in* $p \nmid c$, *kjer je* p *praštevilo, potem velja* $a \equiv b \pmod{p}$.

Dokaz. Iz pogoja $p \nmid c$ in ker je p praštevilo sledi, da je $gcd(c, p) = 1$. Zato po Posledici 2.5 sledi Posledica 2.6. □

Definirajmo kvadratni ostanek ter kvadratni neostanek. Prvi je to terminologijo, prav tako kot kongruenco, vpeljal matematik Carl Friederich Gauss leta 1801 v svojem delu Disquisitiones Arithmeticae. Seveda so se pred njim s tem ukvarjali tudi Fermat, Euler, Lagrange, Legendre ter drugi matematiki s področja teorije števil [1].

Definicija 2.7. [4] Celo število q imenujemo kvadratni ostanek (quadratic residue) po modulu n, če je kongruenten popolnemu kvadratu po modulu n. To pomeni, da obstaja celo število x, tako da $x^2 \equiv q \pmod{n}$. V nasprotnem primeru q imenujemo kvadratni neostanek (quadratic nonresideu) po modulu n .

Legendrovi simboli so poimenovani po francoskem matematiku Adrien Marie Legendre, kateri je definicijo le-teh predstavil v svojem delu Essai sur la Theorie des Nombres [1].

Definicija 2.8. [4] Naj bo p liho praštevilo in a celo število. Potem je Legendrov simbol funkcija števila a in p definirana kot

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{, če je a kvadratni ostanek po modulu p in a} \not\equiv 0 \text{ (mod p)}, \\ -1 & \text{, če je a kvadratni neostanek po modulu p in a} \not\equiv 0 \text{ (mod p)}, \\ 0 & \text{, če je a} \equiv 0 \text{ (mod p)}. \end{cases}$$

Za Legendrove simbole velja kar nekaj lastnosti, katere so predstavljene v naslednjem izreku ter posledici kar je povzeto po [1].

Izrek 2.9. *Naj bo* p *liho praštevilo ter* a *in* b *celi števili tuji* p. *Potem za Legendrove simbole veljajo lastnosti:*

1.

$$\check{C}e\ je\ a \equiv b\ (mod\ p),\ potem\ je\ \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

2.

$$\left(\frac{a^2}{p}\right) = 1.$$

3.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (mod\ p).$$

4.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

5.

$$\left(\frac{1}{p}\right) = 1\ \ in\ \ \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

6.

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$

Dokaz. 1.: Če je $a \equiv b\ (mod\ p)$, potem imata kongruenci $x^2 \equiv a\ (mod\ p)$ in $x^2 \equiv b\ (mod\ p)$ zaradi tranzitivnosti relacije kongruence enaki rešitvi ali pa jih sploh nimata. Torej $x^2 \equiv a\ (mod\ p)$ in $x^2 \equiv b\ (mod\ p)$ sta obe rešljivi ali nobena nima rešitve. Če to poved zapišemo z Legendrovimi simboli dobimo $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2.: Opazimo, da celo število a trivialno zadošča kongruenci $x^2 \equiv a^2\ (mod\ p)$, torej je $\left(\frac{a^2}{p}\right) = 1$.

3.: Posledica Eulerjevega kriterija pravi, da če je p liho praštevilo ter je $gcd(a, p) = 1$, potem je a kvadratni ostanek (oziroma neostanek) po modulu p natanko takrat, ko velja

$$a^{\frac{p-1}{2}} \equiv 1\ (mod\ p)\ (\text{oziroma}\ a^{\frac{p-1}{2}} \equiv -1\ (mod\ p)).$$

Ker velja, da $a \not\equiv 0\ (mod\ p)$ ter je $\left(\frac{a}{p}\right) \equiv 1\ (mod\ p)$ ali $\left(\frac{a}{p}\right) \equiv -1\ (mod\ p)$, sledi, da je

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (mod\ p).$$

4.: Točko 4. dokažemo s pomočjo točke 3.

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\ (mod\ p).$$

Legendrovi simboli zavzamejo vrednosti 1 in -1, torej se nam lahko zgodi, da je $\left(\frac{ab}{p}\right) \neq \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, saj je lahko $1 \equiv -1 \pmod{p}$ ali $2 \equiv 0 \pmod{p}$, vendar samo v primeru, ko je $p < 3$. V našem primeru je p liho praštevilo, torej je $p \geq 3$, zato velja

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

5.: Prvi del $\left(\frac{1}{p}\right) = 1$ je samo poseben primer točke 2., drugi del $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ izpeljemo s pomočjo točke 3. za $a = -1$, torej dobimo $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Oba izraza tako $\left(\frac{-1}{p}\right)$ kot $(-1)^{\frac{p-1}{2}}$ sta enaka 1 ali -1, torej iz kongruence sledi enakost

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

6.: Dokaz sledi neposredno iz točk 2. in 4.

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right).$$

To pomeni, da kvadraten faktor, ki je tuj p, lahko izpustimo v Legendrovih simbolih.

□

Posledica 2.10. *Če je p liho praštevilo, potem velja*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & , \text{ če je } p \equiv 1 \pmod{4}, \\ -1 & , \text{ če je } p \equiv 3 \pmod{4}. \end{cases}$$

Dokaz. Za dokaz uporabimo točko 5. iz Izreka 2.9, torej da je $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Vsako liho praštevilo p je bodisi oblike $4k+1$ bodisi oblike $4k+3$ za neko celo število k. V primeru, ko je oblike $4k+1$ velja

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+1-1}{2}} = (-1)^{\frac{4k}{2}} = (-1)^{2k} = 1.$$

V primeru, ko je oblike $4k+3$ pa velja

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+3-1}{2}} = (-1)^{\frac{4k+2}{2}} = (-1)^{2k+1} = -1.$$

□

Oglejmo si primer uporabe Legendrovih simbolov.

Primer 2.11. Zanima nas ali je kongruenca $x^2 \equiv -46 \pmod{17}$ rešljiva. To pomeni, da moramo izračunati Legendrov simbol $\left(\frac{-46}{17}\right)$. V primeru, da bo rezultat enak 1, bo to pomenilo, da je kongruenca rešljiva, v nasprotnem primeru, če bo rezultat -1, bo

to pomenilo, da kongruenca ni rešljiva.
Upoštevamo točke 4. in 5. iz Izreka 2.9 in dobimo

$$\left(\frac{-46}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{46}{117}\right).$$

Zaradi točke 5. Izreka 2.9 velja $\left(\frac{-1}{17}\right) = (-1)^8 = 1$. Poleg tega vemo, da je $46 \equiv 12 \ (mod\ 17)$, zato po točki 1. velja $\left(\frac{46}{17}\right) = \left(\frac{12}{17}\right)$. Iz tega sledi

$$\left(\frac{-46}{17}\right) = \left(\frac{12}{17}\right).$$

Ob upoštevanju točke 6. Izreka 2.9, saj je $12 = 2^2 \cdot 3$, dobimo $\left(\frac{12}{17}\right) = \left(\frac{3}{17}\right)$. Uporabimo še pravilo iz točke 3. Izreka 2.9, saj sta 3 in 17 tuji števili in dobimo, da je $\left(\frac{3}{17}\right) \equiv 3^{\frac{17-1}{2}} = 3^8 = (3^2)^4 = 9^4 = (9^2)^2 = 81^2 \equiv 13^2 = 169 \equiv -1 \ (mod\ 17)$. Torej je $\left(\frac{-46}{17}\right) = -1$, kar pomeni, da naša kongruenca ni rešljiva. ■

Vrednost Legendrovih simbolov ni potrebno vedno računati s pomočjo kvadratnih ostankov, ampak jih lahko poračunamo s pomočjo štetja ostankov pri deljenju s p, ki ustrezajo določeni lastnosti. S tem se je ukvarjal nemški matematik Gauss. Njegovo odkritje je predstavljeno v Gaussovi lemi.

Lema 2.12. [1] *(GAUSSOVA LEMA) Naj bo p liho praštevilo in $gcd(a, p) = 1$. Če je n število števil iz množice*

$$S = \left\{a, 2a, 3a, \ldots \left(\frac{p-1}{2}\right) a\right\},$$

ki dajo pri deljenju s p ostanek več kot $\frac{p}{2}$, potem velja

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Dokaz. Ker sta a in p tuji števili, nobeno število iz množice S ni kongruentno nič po modulu p, prav tako nobeni dve nista kongruentni po modulu p. Označimo z $r_1, \ldots, r_m$ ostanke števil iz množice S pri deljenju s p, za katere velja $0 < r_i < \frac{p}{2}$ in z $s_1, \ldots, s_n$ ostanke pri deljenju s p, za katere velja $p > s_j > \frac{p}{2}$. Od tod sledi, da je $m + n = \frac{p-1}{2}$ in števila

$$r_1, \ldots, r_m, p - s_1, \ldots, p - s_n$$

so vsa pozitivna in manjša od $\frac{p}{2}$. Če želimo dokazati, da so vsa števila med sabo različna, je dovolj, da dokažemo, da ni nobeno število oblike $p - s_j$ enako kateremukoli številu r_i. To bomo dokazali s protislovjem. Recimo, da obstajata števili i in j, za kateri velja

$$p - s_j = r_i.$$

Potem obstajata celi števili u in v, tako da je $1 \leq u, v \leq \frac{p-1}{2}$ in zadoščata pogojema $s_i \equiv ua \pmod{p}$ ter $r_j \equiv va \pmod{p}$. Torej velja

$$(u+v)a \equiv s_i + r_j \equiv p \equiv 0 \pmod{p},$$

kar pomeni, da je

$$u + v \equiv 0 \pmod{p}, \tag{2.2}$$

saj je $gcd(a, p) = 1$. Vendar enačba (2.2) žal ni rešljiva, saj je $1 < u + v \leq p - 1$. Torej smo prišli do protislovja.
Torej imamo res $\frac{p-1}{2}$ različnih števil

$$r_1, \ldots, r_m, p - s_1, \ldots, p - s_n,$$

ki zavzamejo vrednosti $1, 2, \ldots, \frac{p-1}{2}$, vendar ne nujno v tem vrstnem redu. Njihov produkt je zato enak

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= r_1 \cdots r_m (p - s_1) \cdots (p - s_n) \\ &\equiv r_1 \cdots r_m (-s_1) \cdots (-s_n) \pmod{p} \\ &\equiv (-1)^n r_1 \cdots r_m s_1 \cdots s_n \pmod{p}.\end{aligned}$$

Ampak vemo, da so $r_1, \ldots, r_m, s_1, \ldots, s_n$ kongruentni $a, 2a, \ldots, \frac{p-1}{2}a$ po modulu p, v nekem vrstnem redu, zato velja

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv (-1)^n a \cdot 2a \cdots \frac{p-1}{2} a \pmod{p} \\ &\equiv (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}.\end{aligned}$$

Ker sta $\left(\frac{p-1}{2}\right)!$ in p med saboj tuji števili, lahko kongruenco delimo na obeh straneh s $\left(\frac{p-1}{2}\right)!$ in dobimo

$$1 \equiv (-1)^n a^{\frac{p-1}{2}} \pmod{p}.$$

Kongruenco še malo preoblikujemo, tako da pomnožimo z $(-1)^n$, torej velja

$$(-1)^n \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Po Eulerjevem kriteriju (Izrek 4.12) sledi

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p},$$

torej sledi

$$\left(\frac{a}{p}\right) = (-1)^n.$$

□

Primer 2.13. Izberimo števila $p = 13$ in $a = 7$ ter po Gaussovi lemi (Lema 2.12) izračunajmo Legendrov simbol $\left(\frac{7}{13}\right)$. Ker je $\frac{p-1}{2} = 6$, sledi, da je množica

$$S = \{7, 14, 21, 28, 35, 42\}.$$

Njeni elementi so po modulu 13 enaki

$$7, 1, 8, 2, 9, 4.$$

Torej tri števila iz množice S dajo ostanek pri deljenju s 13 več kot $\frac{13}{2}$, zato po Lemi 2.12 velja

$$\left(\frac{7}{13}\right) = (-1)^3 = -1.$$

■

Izrek 2.14. [1] *Če je p liho praštevilo, potem velja*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & , \text{ če } p \equiv 1 \text{ (mod 8) ali } p \equiv 7 \text{ (mod 8)}, \\ -1 & , \text{ če } p \equiv 3 \text{ (mod 8) ali } p \equiv 5 \text{ (mod 8)}. \end{cases}$$

Dokaz. Po Gaussovi lemi (Lema 2.12) je $\left(\frac{2}{p}\right) = (-1)^n$, kjer je n število elementov množice

$$S = \left\{2, 2 \cdot 2, 3 \cdot 2, \ldots, \left(\frac{p-1}{2}\right) \cdot 2\right\},$$

ki dajo pri deljenju s p ostanek večji od $\frac{p}{2}$. Elementi množice S so vsi manjši od p, zato je dovolj, da preštejemo elemente, ki so po velikosti večji od $\frac{p}{2}$. Za $1 \leq k \leq \frac{p-1}{2}$ je $2k < \frac{p}{2}$, če in samo če, je $k < \frac{p}{4}$. Torej imamo $\lfloor \frac{p}{4} \rfloor$ elementov iz množice S, ki so manjši od $\frac{p}{2}$, zato imamo

$$n = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$$

elementov, ki so večji od $\frac{p}{2}$.
Imamo torej štiri možnosti za liha praštevila, ki so lahko oblike $8k+1, 8k+3, 8k+5$ ali $8k+7$.

$$p = 8k+1 : n = \tfrac{p-1}{2} - \left\lfloor \tfrac{p}{4} \right\rfloor = 4k - \left\lfloor 2k + \tfrac{1}{4} \right\rfloor = 4k - 2k = 2k,$$
$$p = 8k+3 : n = \tfrac{p-1}{2} - \left\lfloor \tfrac{p}{4} \right\rfloor = 4k + 1 - \left\lfloor 2k + \tfrac{3}{4} \right\rfloor = 4k + 1 - 2k = 2k + 1,$$
$$p = 8k+5 : n = \tfrac{p-1}{2} - \left\lfloor \tfrac{p}{4} \right\rfloor = 4k + 2 - \left\lfloor 2k + \tfrac{5}{4} \right\rfloor = 4k + 2 - 2k - 1 = 2k + 1,$$
$$p = 8k+7 : n = \tfrac{p-1}{2} - \left\lfloor \tfrac{p}{4} \right\rfloor = 4k + 3 - \left\lfloor 2k + \tfrac{7}{4} \right\rfloor = 4k + 3 - 2k - 1 = 2k + 2.$$

Torej, če je p oblike $8k+1$ ali $8k+7$, je n sodo število, zato je $\left(\frac{2}{p}\right) = 1$. V primeru, ko je p oblike $8k+3$ ali $8k+5$, je n liho število, zato je $\left(\frac{2}{p}\right) = -1$. □

Posledica 2.15. [1] *Če je p liho praštevilo, potem velja*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Dokaz. Opazimo, da v primeru, ko je p oblike $8k \pm 1$ velja

$$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k,$$

kar je sodo število, zato je $(-1)^{\frac{p^2-1}{8}} = 1 = \left(\frac{2}{p}\right)$. Po drugi strani, ko je p oblike $8k \pm 3$ dobimo

$$\frac{p^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1,$$

kar je liho število, zato je $(-1)^{\frac{p^2-1}{8}} = -1 = \left(\frac{2}{p}\right)$. □

Iz Gaussove leme lahko izpeljemo še enostavnejšo fomulo za izračun Legendrovih simbolov. Povzeto po [1].

Lema 2.16. *Če je p liho praštevilo in a liho celo število, ter velja $gcd(a, p) = 1$, potem je*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor},$$

kjer je $\lfloor \rfloor$ celi del števila.

Dokaz. Definirajmo množico

$$S = \left\{a, 2a, 3a, \ldots \left(\frac{p-1}{2}\right) a\right\}.$$

Vse elemente množice S lahko zapišemo

$$ka = q_k p + t_k,$$

kjer je $1 \leq t_k \leq p-1$. Potem velja $\frac{ka}{p} = q_k + \frac{t_k}{p}$, torej je $\lfloor \frac{ka}{p} \rfloor = q_k$. Zato lahko za $1 \leq k \leq \frac{p-1}{2}$ produkt ka zapišemo kot

$$ka = p\left\lfloor \frac{ka}{p} \right\rfloor + t_k. \tag{2.3}$$

Označimo ostanke pri deljenju s p z $r_1, \ldots, r_m$, za katere velja $0 < r_i < \frac{p}{2}$ in s $s_1, \ldots, s_n$ ostanke pri deljenju s p, za katere velja $p > s_j > \frac{p}{2}$. Torej če je $t_k < \frac{p}{2}$, potem je enako enemu izmed števil $r_1, \ldots, r_m$ oziroma, če je $t_k > \frac{p}{2}$, potem je enako enemu izmed števil $s_1, \ldots, s_n$. Seštejmo elemente množice S ter upoštevajmo enačbo (2.3). Dobimo

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ka}{p} \right\rfloor + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k. \tag{2.4}$$

V Gaussovi lemi (Lema 2.12) smo ugotovili, da so števila

$$r_1, \ldots, r_k, p - s_1, \ldots, p - s_n$$

enaka številom $1, 2, \ldots, \frac{p-1}{2}$ v nekem vrstnem redu. Torej velja

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p - s_k) = pn + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k. \tag{2.5}$$

Če od enačbe (2.4) odštejemo enačbo (2.5) dobimo

$$(a-1)\sum_{k=1}^{\frac{p-1}{2}} k = p\left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - n\right) + 2\sum_{k=1}^{n} s_k. \tag{2.6}$$

Vemo, da je $p \equiv a \equiv 1 \pmod 2$. Poglejmo kongruenco po modulu 2 za enačbo (2.6) ter dobimo

$$0 \cdot \sum_{k=1}^{\frac{p-1}{2}} k \equiv 1 \cdot \left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - n\right) \pmod 2$$

oziroma

$$n \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \pmod 2.$$

Po Gaussovi lemi (Lema 2.12) torej sledi, da je

$$\left(\frac{a}{p}\right) = (-1)^n = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor}.$$

□

Oglejmo si uporabo tega izreka na enakih številih kot v Primeru 2.13.

Primer 2.17. Torej naj bo $p = 13$ in $a = 7$. Za izračun Legendrovega simbola moramo poračunati $\left\lfloor \frac{ka}{p} \right\rfloor$ za $k = 1, 2, \ldots, 6$, saj je $\frac{p-1}{2} = 6$.

$$\left\lfloor \frac{7}{13} \right\rfloor = 0,$$
$$\left\lfloor \frac{14}{13} \right\rfloor = \left\lfloor \frac{21}{13} \right\rfloor = 1,$$
$$\left\lfloor \frac{28}{13} \right\rfloor = \left\lfloor \frac{35}{13} \right\rfloor = 2,$$
$$\left\lfloor \frac{42}{13} \right\rfloor = 3.$$

Torej po Lemi 2.16 je

$$\left(\frac{7}{13}\right) = (-1)^{0+1+1+2+2+3} = (-1)^9 = -1.$$

Torej dobimo res enak rezultat kot v prejšnjem primeru. ■

Naj bosta p in q različni lihi praštevili. Vprašanje, ki se je porajalo matematikom je seveda ali obstaja povezava med Legendrovima simboloma $\left(\frac{p}{q}\right)$ in $\left(\frac{q}{p}\right)$? Oziroma, če poznamo vrednost $\left(\frac{p}{q}\right)$ ali lahko s pomočjo tega izračunamo vrednost $\left(\frac{q}{p}\right)$? Zelo preprosta povezava je najprej uspela švicarskemu matematiku Leonardu Paulu Eulerju leta 1783, katero je nepopolno dokazal Legendre, jo elegantno preoblikov ter poimenoval Quadratic Reciprocity Law. Pod tem imenom jo poznamo še danes. Popoln dokaz je uspel Gaussu, katerega je objavil v svojem delu Disquisitiones Arithmeticae leta 1801. Ravno zaradi tega radi povdarimo, da je to Gaussov zakon kvadratne recipročnosti (Gaussov Quadratic Resiprocity Law) [1].

Izrek 2.18. [1] *(GAUSSOV ZAKON KVADRATNE RECIPROČNOSTI) Naj bosta p in q različni lihi praštevili. Potem za Legendrove simbole velja*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Dokaz. Konstruirajmo pravokotnik z oglišči v točkah $(0,0), (\frac{p}{2}, 0), (0, \frac{q}{2})$ in $(\frac{p}{2}, \frac{q}{2})$. Naj bo R območje znotraj pravokotnika, ki ne vsebuje mejnih črt pravokotnika. Ideja je, da preštejemo točke, katerih koordinate so cela števila, na območju R, na dva različna načina.
Prvi način: p in q sta lihi števili, zato je točk s celoštevilskimi koordinatami (n, m) na območju R s pogojema $1 \leq n \leq \frac{p-1}{2}$ in $1 \leq m \leq \frac{q-1}{2}$ očitno

$$\frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Drugi način: diagonala D pravokotnika, ki poteka od oglišča $(0,0)$ do $(\frac{p}{2}, \frac{q}{2})$, ima enačbo $y = \frac{q}{p}x$, kar je ekvivalentno $py = qx$. Ker je $gcd(p, q) = 1$, nobena točka s celoštevilskimi koordinatami na območju R ne leži na diagonali D, saj p deli x koordinato vsake točke na premici $py = qx$, in q deli y koordinato, ampak takšne točke na območju R ne obstajajo. Naj bo T_1 del območja R, ki je pod diagonalo D, ter T_2 del območja nad diagonalo D. Torej moramo prešteti točke na teh dveh trikotnih območjih. V spodnjem trikotniku velja, da nad vsako točko s koordinatami $(k, 0)$, kjer je k celo število in velja, da je $0 < k \leq \frac{p-1}{2}$, leži $\lfloor \frac{kq}{p} \rfloor$ celoštevilskih točk. Torej vseh celoštevilskih točk v območju T_1 je

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor.$$

Na podoben način preštejemo točke na območju T_2, katerih je

$$\sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor.$$

Vseh točk na območju R je torej vsota števila točk na območju T_1 ter števila točk na območju T_2.
Torej, če primerjamo obe štetji točk na območju R dobimo

$$\frac{p-1}{2}\cdot\frac{q-1}{2}=\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{kq}{p}\right\rfloor+\sum_{j=1}^{\frac{q-1}{2}}\left\lfloor\frac{jp}{q}\right\rfloor.$$

Po Lemi 2.16 torej sledi

$$\begin{aligned}\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) &= (-1)^{\sum_{j=1}^{\frac{q-1}{2}}\lfloor\frac{jp}{q}\rfloor}\cdot(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\lfloor\frac{kq}{p}\rfloor}\\ &= (-1)^{\sum_{j=1}^{\frac{q-1}{2}}\lfloor\frac{jp}{q}\rfloor+\sum_{k=1}^{\frac{p-1}{2}}\lfloor\frac{kq}{p}\rfloor}\\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.\end{aligned}$$

□

Iz Gaussovega izreka izpeljemo dve posledici, ki nam olajšata računanje Legendrovih simbolov in sta odvisni od števil p in q. Pomembno je ali sta to lihi praštevili, ki data pri deljenju s 4 ostanek 1 ali 3. Obe posledici sta povzeti po [1].

Posledica 2.19. *Če sta p in q različni lihi praštevili, potem velja*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\begin{cases}1 & , \text{ če } p\equiv 1 \pmod 4 \text{ ali } q\equiv 1 \pmod 4,\\ -1 & , \text{ če } p\equiv q\equiv 3 \pmod 4.\end{cases}$$

Dokaz. Po Izreku 2.18 velja

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Če je p kongruenten 1 po modulu 4, potem je $p=4k+1$, zato je $\frac{p-1}{2}=2k$, torej je sodo število. Enako velja za q, če je kongruenten 1 po modulu 4, potem je $q=4l+1$, zato je $\frac{q-1}{2}=2l$, prav tako sodo število. Če je vsaj eden izmed p in q kongruenten 1 po modulu 4, je vsaj eden izmed ulomkov $\frac{p-1}{2}$ in $\frac{q-1}{2}$ sodo število, zato je njun produkt sodo število in je $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}=1$.
Če sta oba tako p kot q kongruentna 3 po modulu 4, velja da sta oblike $p=4k+3$ in $q=4l+3$, torej velja

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}=(-1)^{\frac{4k+3-1}{2}\frac{4l+3-1}{2}}=(-1)^{(2k+1)(2l+1)}=-1,$$

saj je produkt dveh lihih števil liho število. □

Primer 2.20. Oglejmo si izračun produkta $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$ za $p = 7$ in $q = 11$. Najprej si poglejmo izračun po definiciji.

$$\left(\frac{7}{11}\right) = -1,$$

saj 7 ni kvadratni ostanek od 11.

$$n \equiv 1 \ (mod\ 11) \Rightarrow n^2 \equiv 1 \ (mod\ 11),$$

$$n \equiv 2 \ (mod\ 11) \Rightarrow n^2 \equiv 4 \ (mod\ 11),$$

$$n \equiv 3 \ (mod\ 11) \Rightarrow n^2 \equiv 9 \ (mod\ 11),$$

$$n \equiv 4 \ (mod\ 11) \Rightarrow n^2 \equiv 5 \ (mod\ 11),$$

$$n \equiv 5 \ (mod\ 11) \Rightarrow n^2 \equiv 3 \ (mod\ 11),$$

$$n \equiv 6 \ (mod\ 11) \Rightarrow n^2 \equiv 3 \ (mod\ 11),$$

$$n \equiv 7 \ (mod\ 11) \Rightarrow n^2 \equiv 5 \ (mod\ 11),$$

$$n \equiv 8 \ (mod\ 11) \Rightarrow n^2 \equiv 4 \ (mod\ 11),$$

$$n \equiv 9 \ (mod\ 11) \Rightarrow n^2 \equiv 9 \ (mod\ 11),$$

$$n \equiv 10 \ (mod\ 11) \Rightarrow n^2 \equiv 1 \ (mod\ 11).$$

Kvadrat naravnega števila je lahko kongruenten samo $0, 1, 3, 4, 5$ ali 9 po modulu 11.

$$\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = 1,$$

saj je $11 \equiv 4 \ (mod\ 7)$ in po točki 1. Izreka 2.9 velja $\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right)$. Ker velja $2^2 \equiv 4 \ (mod\ 7)$, pomeni, da je 4 kvadratni ostanek od 7, zato je $\left(\frac{4}{7}\right) = 1$. Torej je produkt enak

$$\left(\frac{7}{11}\right)\left(\frac{11}{7}\right) = (-1) \cdot 1 = -1.$$

Po Posledici 2.19 velja

$$\left(\frac{7}{11}\right)\left(\frac{11}{7}\right) = -1,$$

saj sta $p = 7$ in $q = 11$ kongruentna 3 po modulu 4. V obeh primerih smo dobili enak rezultat, vendar je bil izračun v drugem primeru bistveno hitrejši. ■

Posledica 2.21. *Če sta p in q različni lihi praštevili, potem velja*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & , \text{ če } p \equiv 1 \ (mod\ 4) \text{ ali } q \equiv 1 \ (mod\ 4), \\ -\left(\frac{q}{p}\right) & , \text{ če } p \equiv q \equiv 3 \ (mod\ 4). \end{cases}$$

Dokaz. Po Izreku 2.18 velja

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Enačbo pomnožimo s $\left(\frac{q}{p}\right)$ in dobimo

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Upoštevamo, da je $\left(\frac{q}{p}\right)^2 = 1$ ter dobimo

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Če upoštevamo Posledico 2.19, dobimo, da je $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ v primeru, ko je p kongruenten 1 po modulu 4 ali q kongruenten 1 po modulu 4, ter $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ v primeru, ko sta p in q kongruentna 3 po modulu 4. □

Posplošitev Legendrovih simbolov so Jacobijevi simboli. Karl Gustav Jacob Jacobi je bil nemški matematik, ki je deloval na področju eliptičnih funkcij, diferencialnih enačbah, teoriji števil...

Definicija 2.22. [4] Za vsako celo število a in pozitivno liho število n je Jacobijev simbol $\left(\frac{a}{n}\right)$ definiran kot produkt Legendrovih simbolov, ki predstavljajo praštevilski razcep števila n

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\cdots\left(\frac{a}{p_k}\right)^{\alpha_k},$$

kjer je $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ praštevilski razcep števila n.

Primer 2.23. Izračunajmo Jacobijev simbol $\left(\frac{7}{90}\right)$. Ker je $90 = 5 \cdot 3^2 \cdot 2$ po Definiciji 2.22 velja

$$\left(\frac{7}{90}\right) = \left(\frac{7}{5}\right)\left(\frac{7}{3}\right)^2\left(\frac{7}{2}\right).$$

Posebej poračunamo te tri Legendrove simbole. Ker je $7 \equiv 2 \ (mod\ 5)$, velja da je $\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right)$ po točki 1. Izreka 2.9.

$$n = 1 : n \equiv 1 \ (mod\ 5) \Rightarrow n^2 \equiv 1 \ (mod\ 5),$$

$$n = 2 : n \equiv 2 \ (mod\ 5) \Rightarrow n^2 \equiv 4 \ (mod\ 5),$$

$$n = 3 : n \equiv 3 \ (mod\ 5) \Rightarrow n^2 \equiv 4 \ (mod\ 5),$$

$$n = 4 : n \equiv 4 \ (mod\ 5) \Rightarrow n^2 \equiv 1 \ (mod\ 5).$$

Torej 2 ni kvadratni ostanek od 5, saj ne obstaja kvadrat celega števila, ki bi bil kongruenten 2 po modulu 5, zato je $\left(\frac{2}{5}\right) = -1$.

$7 \equiv 1 \ (mod\ 3)$ in vemo, da je $1^2 \equiv 1 \ (mod\ 3)$, torej je 1 kvadratni ostanek od 3, zato velja

$$\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Podobno velja tudi za zadnji simbol. $7 \equiv 1 \ (mod\ 2)$ in vemo, da je $1^2 \equiv 1 \ (mod\ 2)$, torej je 1 kvadratni ostanek od 2, zato velja

$$\left(\frac{7}{2}\right) = \left(\frac{1}{2}\right) = 1.$$

Iz tega sledi

$$\left(\frac{7}{90}\right) = (-1) \cdot 1^2 \cdot 1 = -1.$$

■

Za Jacobijeve simbole veljajo podobne zveze kot za Legendrove simbole. Nekaj najbolj uporabnih je predstavljeno v naslednjih izrekih.

Lema 2.24. *Naj bodo a, b in n poljubna cela števila in $n \geq 1$. Če sta a in b kongruentni po modulu n, potem velja*

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right).$$

Dokaz. Po definiciji velja

$$\left(\frac{a}{n}\right) = \left(\frac{a}{n_1}\right)^{\alpha_1} \left(\frac{a}{n_2}\right)^{\alpha_2} \cdots \left(\frac{a}{n_k}\right)^{\alpha_k} \tag{2.7}$$

in

$$\left(\frac{b}{n}\right) = \left(\frac{b}{n_1}\right)^{\alpha_1} \left(\frac{b}{n_2}\right)^{\alpha_2} \cdots \left(\frac{b}{n_k}\right)^{\alpha_k} \tag{2.8}$$

za praštevilski rezcep $n = n_1^{\alpha_1} n_2^{\alpha_2} \cdots n_k^{\alpha_k}$. Ker velja, da je

$$a \equiv b \ (mod\ n)$$

velja tudi

$$a \equiv b \ (mod\ n_1),$$
$$a \equiv b \ (mod\ n_2),$$
$$\vdots$$
$$a \equiv b \ (mod\ n_k).$$

Torej sta a in b oba hkrati kvadratna ostanka ali kvadratna neostanka po modulu n_1, zato sta vrednosti Legendrovih simbolov enaki, torej

$$\left(\frac{a}{n_1}\right) = \left(\frac{b}{n_1}\right).$$

Enako velja za vse ostale člene produkta v enačbah (2.7) in (2.8). Zato velja

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right).$$

□

Izrek 2.25. [4] *Naj bosta x in y celi števili ter p in r lihi pozitivni števili. Potem velja*

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \tag{2.9}$$

in

$$\left(\frac{x}{pr}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{r}\right). \tag{2.10}$$

Dokaz. (2.9): Recimo, da je p liho praštevilo in naj bo R množica vseh kvadratnih ostankov od p, ki so tuja p, ter N množica vseh kavdratnih neostankov od p, ki so pravtako tuji p. Naj bo $m = \frac{p-1}{2}$. Potem obstaja natanko m kongruenčnih razredov števil, ki so tuja p ter so kvadratni ostanek od p. Naj te kongruenčne razrede predstavljajo števila $r_1, r_2, \ldots, r_m$, kjer $r_j \not\equiv r_j \pmod{p}$, ko je $i \neq j$. Seveda obstaja tudi natanko m kongrunčnih razredov števil, ki so tuja p ter so kvadratni neostanek od p.
Produkt dveh kvadratnih ostankov od p je pravtako kvadratni ostanek od p. Torej velja $xy \in R$ za vsak $x \in R$ in $y \in R$. Zato za Legendrove simbole velja $\left(\frac{xy}{p}\right) = 1$, $\left(\frac{x}{p}\right) = 1$ in $\left(\frac{y}{p}\right) = 1$, torej velja $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.
Recimo, da je $x \in R$. Potem $xr_i \in R$ za vsak $i = 1, 2, \ldots m$, in $xr_i \not\equiv xr_j \pmod{p}$, ko $r_i \neq r_j$. Iz tega sledi, da so kongruenčni razredi $xr_1, xr_2, \ldots, xr_m$ različni in vsebujejo kvadratne ostanke od p. To pomeni, da je vsak kvadratni ostanek od p kongruenten natanko enemu številu $xr_1, xr_2, \ldots, xr_m$. Ampak, če je $y \in N$, potem $y \not\equiv r_i \pmod{p}$, torej tudi $xy \not\equiv xr_i \pmod{p}$ za vsak $i = 1, 2, \ldots, m$. To pomeni, da $xy \in N$ za vsak $x \in R$ in $y \in N$. Zato za Legendrove simbole velja $\left(\frac{xy}{p}\right) = -1$, $\left(\frac{x}{p}\right) = 1$ in $\left(\frac{y}{p}\right) = -1$, torej velja $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.
Predpostavimo, da je $x \in N$. Potem je $xr_i \in N$ za vsak $i = 1, 2, \ldots, m$, in $xr_i \not\equiv xr_j \pmod{p}$, ko velja $i \neq j$. Iz tega sledi, da so kongruenčni razredi $xr_1, xr_2, \ldots, xr_m$ različni in vsebujejo kvadratne neostanke po modulu p. Ampak kongruenčnih razredov od kvadratnih neneostankov je netanko m, torej sledi, da je vsak kvadratni neostanek od p kongruenten natanko enem izmed števil $xr_1, xr_2, \ldots, xr_m$. Ampak, če je $y \in N$, potem $y \not\equiv r_i \pmod{p}$, ko je $xy \not\equiv xr_i \pmod{p}$ za $i = 1, 2, \ldots m$. Torej sledi, da $xy \in R$ za vsak $x \in N$ in $y \in N$. Zato za Legendrove simbole velja $\left(\frac{xy}{p}\right) = 1$, $\left(\frac{x}{p}\right) = -1$ in $\left(\frac{y}{p}\right) = -1$, torej velja $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.
Po definiciji so Jacobijevi simboli, samo produkt Legendrovih simbolov

$$\left(\frac{x}{p}\right) = \left(\frac{x}{p_1}\right)^{\alpha_1}\left(\frac{x}{p_2}\right)^{\alpha_2}\cdots\left(\frac{x}{p_k}\right)^{\alpha_k},$$

kjer je $p = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ torej je naša formula

$$\left(\frac{xy}{p_1}\right)^{\alpha_1} \left(\frac{xy}{p_2}\right)^{\alpha_2} \cdots \left(\frac{xy}{p_k}\right)^{\alpha_k} = \left(\frac{x}{p_1}\right)^{\alpha_1} \left(\frac{x}{p_2}\right)^{\alpha_2} \cdots \left(\frac{x}{p_k}\right)^{\alpha_k} \left(\frac{y}{p_1}\right)^{\alpha_1} \left(\frac{y}{p_2}\right)^{\alpha_2} \cdots \left(\frac{y}{p_k}\right)^{\alpha_k}.$$

Za vsak p_i velja $\left(\frac{xy}{p_i}\right)^{\alpha_i} = \left(\frac{x}{p_i}\right)^{\alpha_i} \left(\frac{y}{p_i}\right)^{\alpha_i}$, torej velja tudi naša formula.

(2.10): Dokaz sledi neposredno iz definicije.

$$\left(\frac{x}{pr}\right) = \left(\frac{x}{p_1}\right)^{\alpha_1} \left(\frac{x}{p_2}\right)^{\alpha_2} \cdots \left(\frac{x}{p_k}\right)^{\alpha_k} \left(\frac{x}{r_1}\right)^{\beta_1} \left(\frac{x}{r_2}\right)^{\beta_2} \cdots \left(\frac{x}{r_l}\right)^{\beta_l},$$

kjer sta $p = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ in $r = r_1^{\beta_1} r_2^{\beta_2} \cdots r_l^{\beta_l}$ praštevilska razcepa za števili p in r. Prvih k členov je po definiciji enaki $\left(\frac{x}{p}\right)$, naslednjih l členov pa $\left(\frac{x}{r}\right)$. Torej je

$$\left(\frac{x}{pr}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{r}\right).$$

□

Izrek 2.26. *Naj bosta m in n dve lihi tuji celi števili. Potem velja*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Dokaz. Naj bo

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} q_1^{\beta_1} q_2^{\beta_2} \cdots q_j^{\beta_j}$$

praštevilski razcep števila m, kjer je p_t praštevilo kongruentno 1 po modulu 4 za vsak $t \in \{1, 2, \ldots, i\}$, ter q_u praštevilo kongruentno 3 po modulu 4 za vsak $u \in \{1, 2, \ldots, j\}$. Naj bo

$$n = r_1^{\gamma_1} r_2^{\gamma_2} \cdots r_k^{\gamma_k} s_1^{\delta_1} s_2^{\delta_2} \cdots s_l^{\delta_l}$$

praštevilski razcep števila n, kjer je r_v praštevilo kongruentno 1 po modulu 4 za vsak $v \in \{1, 2, \ldots, k\}$, ter s_z praštevilo kongruentno 3 po modulu 4 za vsak $z \in \{1, 2, \ldots, l\}$. Naj bosta a in b celi števili kongruentni 1 po modulu 4, ter c in d celi števili kongruentni 3 po modulu 4. Potem velja:

$$a \equiv 1 \pmod 4 \text{ in } b \equiv 1 \pmod 4 \Rightarrow ab \equiv 1 \pmod 4,$$

$$c \equiv 3 \pmod 4 \text{ in } d \equiv 3 \pmod 4 \Rightarrow cd \equiv 9 \equiv 1 \pmod 4,$$

$$a \equiv 1 \pmod 4 \text{ in } c \equiv 3 \pmod 4 \Rightarrow ac \equiv 3 \pmod 4.$$

Torej če sta obe števili konkruentni bodisi 1 bodisi 3 po modulu 4, potem je njun produkt kongruenten 1 po modulu 4. V primeru, ko pa je eno število kongruentno 1 ter

drugo kongruentno 3 po modulu 4, potem je njun produkt kongruenten 3 po modulu 4.

Torej za število m velja

$$m \equiv 3 \ (mod\ 4) \quad \Leftrightarrow \quad \beta_1 + \beta_2 + \cdots + \beta_j \ \textit{liho število,}$$

ter za število n velja

$$n \equiv 3 \ (mod\ 4) \quad \Leftrightarrow \quad \delta_1 + \delta_2 + \cdots + \delta_l \ \textit{liho število.}$$

Sedaj si oglejmo produkt Jacobijevih simbolov.

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \left(\frac{m}{r_1^{\gamma_1} r_2^{\gamma_2} \cdots r_k^{\gamma_k} s_1^{\delta_1} s_2^{\delta_2} \cdots s_l^{\delta_l}}\right)\left(\frac{n}{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} q_1^{\beta_1} q_2^{\beta_2} \cdots q_j^{\beta_j}}\right) =$$

$$\left(\frac{m}{r_1}\right)^{\gamma_1} \cdots \left(\frac{m}{r_k}\right)^{\gamma_k} \left(\frac{m}{s_1}\right)^{\delta_1} \cdots \left(\frac{m}{s_l}\right)^{\delta_l} \left(\frac{n}{p_1}\right)^{\alpha_1} \cdots \left(\frac{n}{p_i}\right)^{\alpha_i} \left(\frac{n}{q_1}\right)^{\beta_1} \cdots \left(\frac{n}{q_j}\right)^{\beta_j}. \quad (2.11)$$

Enačba (2.11) velja zaradi točke (2.10) Izreka 2.25. Če upoštevamo še točko (2.9) Izreka 2.25 za posamezen člen produkta v enačbi (2.11) dobimo

$$\begin{aligned} \left(\frac{m}{r_1}\right)^{\gamma_1} &= \left(\left(\frac{p_1}{r_1}\right)^{\alpha_1} \cdots \left(\frac{p_i}{r_1}\right)^{\alpha_i} \left(\frac{q_1}{r_1}\right)^{\beta_1} \cdots \left(\frac{q_j}{r_1}\right)^{\beta_j}\right)^{\gamma_1} = \qquad (2.12) \\ &= \left(\frac{p_1}{r_1}\right)^{\alpha_1\gamma_1} \cdots \left(\frac{p_i}{r_1}\right)^{\alpha_i\gamma_1} \left(\frac{q_1}{r_1}\right)^{\beta_1\gamma_1} \cdots \left(\frac{q_j}{r_1}\right)^{\beta_j\gamma_1} \end{aligned}$$

$$\vdots$$

$$\begin{aligned} \left(\frac{m}{r_k}\right)^{\gamma_k} &= \left(\left(\frac{p_1}{r_k}\right)^{\alpha_1} \cdots \left(\frac{p_i}{r_k}\right)^{\alpha_i} \left(\frac{q_1}{r_k}\right)^{\beta_1} \cdots \left(\frac{q_j}{r_k}\right)^{\beta_j}\right)^{\gamma_k} = \qquad (2.13) \\ &= \left(\frac{p_1}{r_k}\right)^{\alpha_1\gamma_k} \cdots \left(\frac{p_i}{r_k}\right)^{\alpha_i\gamma_k} \left(\frac{q_1}{r_k}\right)^{\beta_1\gamma_k} \cdots \left(\frac{q_j}{r_k}\right)^{\beta_j\gamma_k} \end{aligned}$$

$$\vdots$$

$$\begin{aligned} \left(\frac{n}{q_1}\right)^{\beta_1} &= \left(\left(\frac{r_1}{q_1}\right)^{\gamma_1} \cdots \left(\frac{r_k}{q_1}\right)^{\gamma_k} \left(\frac{s_1}{q_1}\right)^{\delta_1} \cdots \left(\frac{s_l}{q_1}\right)^{\delta_l}\right)^{\beta_1} = \qquad (2.14) \\ &= \left(\frac{r_1}{q_1}\right)^{\gamma_1\beta_1} \cdots \left(\frac{r_k}{q_1}\right)^{\gamma_k\beta_1} \left(\frac{s_1}{q_1}\right)^{\delta_1\beta_1} \cdots \left(\frac{s_l}{q_1}\right)^{\delta_l\beta_1} \end{aligned}$$

$$\vdots$$

$$\begin{aligned} \left(\frac{n}{q_j}\right)^{\beta_j} &= \left(\left(\frac{r_1}{q_j}\right)^{\gamma_1} \cdots \left(\frac{r_k}{q_j}\right)^{\gamma_k} \left(\frac{s_1}{q_j}\right)^{\delta_1} \cdots \left(\frac{s_l}{q_j}\right)^{\delta_l}\right)^{\beta_j} = \qquad (2.15) \\ &= \left(\frac{r_1}{q_j}\right)^{\gamma_1\beta_j} \cdots \left(\frac{r_k}{q_j}\right)^{\gamma_k\beta_j} \left(\frac{s_1}{q_j}\right)^{\delta_1\beta_j} \cdots \left(\frac{s_l}{q_j}\right)^{\delta_l\beta_j}. \end{aligned}$$

Če upoštevamo zgornje enakosti ((2.12), (2.13), (2.14), (2.15)) v enačbi (2.11) dobimo

$$\begin{aligned}\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \left(\frac{p_1}{r_1}\right)^{\alpha_1\gamma_1}\left(\frac{r_1}{p_1}\right)^{\gamma_1\alpha_1}\left(\frac{p_1}{r_2}\right)^{\alpha_1\gamma_2}\left(\frac{r_2}{p_1}\right)^{\gamma_2\alpha_1}\cdots\left(\frac{s_l}{q_j}\right)^{\delta_j\beta_l}\left(\frac{q_j}{s_l}\right)^{\beta_l\delta_j} \quad (2.16)\\ &= \left(\left(\frac{p_1}{r_1}\right)\left(\frac{r_1}{p_1}\right)\right)^{\alpha_1\gamma_1}\left(\left(\frac{p_1}{r_2}\right)\left(\frac{r_2}{p_1}\right)\right)^{\alpha_1\gamma_2}\cdots\left(\left(\frac{s_l}{q_j}\right)\left(\frac{q_j}{s_l}\right)\right)^{\beta_l\delta_j}.\end{aligned}$$

Veliko členov produkta v enačbi (2.16) je po Gaussovem zakonu kvadratne recipročnosti (Izrek 2.18) enako 1. Ostanejo nam samo členi, v katerih sta obe števili v Jacobijevem simbolu kongruentni 3 po modulu 4. Za te člene prav tako po Gussovem zakonu kvadratne recipročnocti (Izrek 2.18) velja, da so enaki -1.

$$\begin{aligned}\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \left(\left(\frac{q_1}{s_1}\right)\left(\frac{s_1}{q_1}\right)\right)^{\beta_1\delta_1}\left(\left(\frac{q_2}{s_1}\right)\left(\frac{s_1}{q_2}\right)\right)^{\beta_2\delta_1}\cdots\left(\left(\frac{q_j}{s_l}\right)\left(\frac{s_l}{q_j}\right)\right)^{\beta_j\delta_l}\\ &= (-1)^{\beta_1\delta_1}(-1)^{\beta_2\delta_1}\cdots(-1)^{\beta_j\delta_1}(-1)^{\beta_1\delta_2}(-1)^{\beta_2\delta_2}\cdots(-1)^{\beta_j\delta_l}\\ &= (-1)^{\beta_1\delta_1+\beta_2\delta_1+\cdots+\beta_j\delta_1+\beta_1\delta_2+\beta_2\delta_2+\cdots+\beta_j\delta_l}\\ &= (-1)^{(\beta_1+\beta_2\cdots+\beta_j)(\delta_1+\delta_2+\cdots+\delta_l)}.\end{aligned}$$

Produkt je torej bodisi enak 1 bodisi enak -1.

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \begin{cases} 1 & , \beta_1+\cdots+\beta_j \text{ je sodo število ali } \delta_1+\cdots+\delta_l \text{ je sodo število} \quad (2.17)\\ -1 & , \beta_1+\cdots+\beta_j \text{ in } \delta_1+\cdots+\delta_l \text{ sta lihi števili.} \quad (2.18)\end{cases}$$

Pogoj (2.17) velja natanko tedaj, ko je ali m ali n kongruenten 1 po modulu 4. V tem primeru je tudi

$$(-1)^{\frac{m-1}{2}\frac{n-1}{2}} = 1,$$

saj je vsaj eden izmed $\frac{m-1}{2}$ ali $\frac{n-1}{2}$ sodo število.
Pogoj (2.18) velja natako tedaj, ko sta m in n kongruentni 3 po modulu 4. V tem primeru je tudi

$$(-1)^{\frac{m-1}{2}\frac{n-1}{2}} = -1,$$

saj sta $\frac{m-1}{2}$ in $\frac{n-1}{2}$ lihi števili, torej je tudi njun produkt liho število.
Torej res velja, da je $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$. □

Izrek 2.27. [4]

$$\left(\frac{-1}{s}\right) = (-1)^{\frac{s-1}{2}}$$

za vsa liha pozitivna cela števila s.

Dokaz. Naj bo $f(s) = (-1)^{\frac{s-1}{2}} \cdot \left(\frac{-1}{s}\right)$ za vsako liho pozitivno število s. Dokazati moramo, da je $f(s) = 1$ za vsako liho pozitivno število. Če sta s in t lihi pozitivni števili, potem velja

$$(st-1)-(s-1)-(t-1) = st-s-t+1 = (s-1)(t-1).$$

Ampak produkt $(s-1)(t-1)$ je deljiv s 4, saj sta s in t lihi pozitivni števili, torej sta člena produkta $(s-1)$ in $(t-1)$ sodi števili. Torej sledi, da

$$\frac{st-1}{2} \equiv \frac{s-1}{2} + \frac{t-1}{2} \pmod 2$$

iz česar sledi

$$(-1)^{\frac{st-1}{2}} = (-1)^{\frac{s-1}{2}} \cdot (-1)^{\frac{t-1}{2}}. \tag{2.19}$$

Ob upoštevanju Izreka 2.25 ter enačbe (2.19), sledi da je $f(st) = f(s)f(t)$ za vsa liha števila s in t. Če je p liho praštevilo, potem po točki 5. Izreka 2.9 velja $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, torej sta člena $\left(\frac{-1}{p}\right)$ in $(-1)^{\frac{p-1}{2}}$ bodisi oba 1 bodisi oba -1, torej je njun produkt vedno 1. Iz tega sledi, da je $f(s) = 1$ za vsa liha pozitivna števil s. □

Izrek 2.28. [4]

$$\left(\frac{2}{s}\right) = (-1)^{\frac{s^2-1}{8}}$$

za vsa liha pozitivna števila s.

Dokaz. Naj bo $g(s) = (-1)^{\frac{s^2-1}{8}} \cdot \left(\frac{2}{s}\right)$ za vsa liha pozitivna števila s. Dokazati moramo, da je $g(s) = 1$ za vsako liho pozitivno število s. Če sta s in t lihi pozitivni števili, potem velja

$$(s^2t^2-1) - (s^2-1) - (t^2-1) = s^2t^2 - s^2 - t^2 + 1 = (s^2-1)(t^2-1).$$

Produkt $(s^2-1)(t^2-1)$ je deljiv s 64, saj je kvadrat vsakega lihega števila kongruenten 1 po modulu 8, torej sta člena (s^2-1) in (t^2-1) oba deljiva z 8. Iz tega sledi, da je

$$\frac{s^2t^2-1}{8} \equiv \frac{s^21}{8}\frac{t^2-1}{8} \pmod 8,$$

torej velja

$$(-1)^{\frac{s^2t^2-1}{8}} = (-1)^{\frac{s^2-1}{8}}(-1)^{\frac{t^2-1}{8}}. \tag{2.20}$$

Ob upoštevanju Izreka 2.25 ter enačbe (2.20), sledi da je $g(st) = g(s)g(t)$ za vsa liha števila s in t. Če je p liho praštevilo, potem po Posledici 2.15 velja $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, torej sta člena $\left(\frac{2}{p}\right)$ in $(-1)^{\frac{p^2-1}{8}}$ bodisi oba 1 bodisi oba -1, torej je njun produkt vedno 1. Iz tega sledi, da je $g(s) = 1$ za vsa liha pozitivna števil s.

□

Izrek 2.29. [4] *Če je $b \equiv 1$ ali $3 \pmod 8$, potem za Jacobijev simbol velja*

$$\left(\frac{-2}{b}\right) = 1.$$

Dokaz. Upoštevamo pravilo iz Izreka 2.25, torej velja

$$\left(\frac{-2}{b}\right) = \left(\frac{-1}{b}\right)\left(\frac{2}{b}\right). \tag{2.21}$$

Upoštevamo še Izrek 2.27 ter Izrek 2.28, torej po enačbi (2.21) dobimo

$$\left(\frac{-2}{b}\right) = (-1)^{\frac{b-1}{2}} \cdot (-1)^{\frac{b^2-1}{8}} = (-1)^{\frac{b-1}{2}+\frac{b^2-1}{8}}. \tag{2.22}$$

Oglejmo si vsoto $\frac{b-1}{2} + \frac{b^2-1}{8}$. Če je $b = 8k+1$, potem velja

$$\begin{aligned}
\frac{b-1}{2} + \frac{b^2-1}{8} &= \frac{8k+1-1}{2} + \frac{(8k+1)^2-1}{8} \\
&= \frac{8k}{2} + \frac{64k^2+16k+1-1}{8} \\
&= 4k + \frac{64k^2+16k}{8} \\
&= 4k + 8k^2 + 2k \\
&= 8k^2 + 6k \\
&= 2(4k^2+3k).
\end{aligned}$$

Če je $b = 8k+3$, potem velja

$$\begin{aligned}
\frac{b-1}{2} + \frac{b^2-1}{8} &= \frac{8k+3-1}{2} + \frac{(8k+3)^2-1}{8} \\
&= \frac{8k+2}{2} + \frac{64k^2+48k+9-1}{8} \\
&= 4k+1 + \frac{64k^2+48k+8}{8} \\
&= 4k+1+8k^2+6k+1 \\
&= 8k^2+10k+2 \\
&= 2(4k^2+5k+1).
\end{aligned}$$

V obeh primerih je vsota sodo število, torej po enačbi (2.22) dobimo, da je

$$\left(\frac{-2}{b}\right) = 1.$$

□

Primer 2.30. Preverimo ali je 444 kvadratni ostanek praštevila 751.

$$\left(\frac{444}{751}\right) = \left(\frac{2}{751}\right)^2 \left(\frac{111}{751}\right),$$

zaradi Izreka 2.25. $\left(\frac{2}{751}\right) = (-1)^{\frac{751^2-1}{8}} = 1$, po Izreku 2.28, ter $\left(\frac{111}{751}\right) = (-1)^{\frac{110\cdot 750}{4}} \left(\frac{751}{111}\right) = (-1)\left(\frac{751}{111}\right)$, po Izreku 2.18. Torej sledi, da je

$$\left(\frac{444}{751}\right) = (-1)\left(\frac{751}{111}\right).$$

Ker je $751 \equiv 85 \pmod{111}$, velja da je $\left(\frac{751}{111}\right) = \left(\frac{85}{111}\right)$, kar je pa enako $(-1)^{\frac{84\cdot 110}{4}} \left(\frac{111}{85}\right) = \left(\frac{111}{85}\right)$, zaradi Izreka 2.18. Torej velja

$$\left(\frac{444}{751}\right) = (-1)\left(\frac{111}{85}\right).$$

Upoštevamo, da je $111 \equiv 26 \pmod{85}$ ter, da je $26 = 2 \cdot 13$, torej po Izreku 2.25 sledi

$$\left(\frac{444}{751}\right) = (-1)\left(\frac{2}{85}\right)\left(\frac{13}{85}\right).$$

Po Izreku 2.28 velja, da je $\left(\frac{2}{85}\right) = (-1)^{\frac{85^2-1}{8}} = -1$, ter po Izreku 2.18 sledi, da je $\left(\frac{13}{85}\right) = (-1)^{\frac{12\cdot 84}{4}} \left(\frac{85}{13}\right) = \left(\frac{85}{13}\right)$. Torej velja

$$\left(\frac{444}{751}\right) = (-1)(-1)\left(\frac{85}{13}\right) = \left(\frac{85}{13}\right).$$

Poglejmo si kongruence popolnih kvadratov po modulu 13 :

$$\begin{aligned}
n = 1: &\quad n \equiv 1 \pmod{13} \Rightarrow n^2 \equiv 1 \pmod{13},\\
n = 2: &\quad n \equiv 2 \pmod{13} \Rightarrow n^2 \equiv 4 \pmod{13},\\
n = 3: &\quad n \equiv 3 \pmod{13} \Rightarrow n^2 \equiv 9 \pmod{13},\\
n = 4: &\quad n \equiv 4 \pmod{13} \Rightarrow n^2 \equiv 3 \pmod{13},\\
n = 5: &\quad n \equiv 5 \pmod{13} \Rightarrow n^2 \equiv 12 \pmod{13},\\
n = 6: &\quad n \equiv 6 \pmod{13} \Rightarrow n^2 \equiv 10 \pmod{13},\\
n = 7: &\quad n \equiv 7 \pmod{13} \Rightarrow n^2 \equiv 10 \pmod{13},\\
n = 8: &\quad n \equiv 8 \pmod{13} \Rightarrow n^2 \equiv 12 \pmod{13},\\
n = 9: &\quad n \equiv 9 \pmod{13} \Rightarrow n^2 \equiv 3 \pmod{13},\\
n = 10: &\quad n \equiv 10 \pmod{13} \Rightarrow n^2 \equiv 9 \pmod{13},\\
n = 11: &\quad n \equiv 11 \pmod{13} \Rightarrow n^2 \equiv 4 \pmod{13},\\
n = 12: &\quad n \equiv 12 \pmod{13} \Rightarrow n^2 \equiv 1 \pmod{13},\\
n = 13: &\quad n \equiv 0 \pmod{13} \Rightarrow n^2 \equiv 0 \pmod{13}.
\end{aligned}$$

Ker je $85 \equiv 7 \pmod{13}$ velja, da je $\left(\frac{85}{13}\right) = \left(\frac{7}{13}\right) = -1$, ker 7 ni kvadratni ostanek od 13, saj ne obstaja celo število a, da bi veljalo $a^2 \equiv 7 \pmod{13}$. Torej je

$$\left(\frac{444}{751}\right) = -1,$$

kar pomeni, da 444 ni kvadratni ostanek praštevila 751. ■

3 PREDSTAVITEV NARAVNIH ŠTEVIL KOT VSOTE DVEH KVADRATOV

Nekatera naravna števila lahko predstavimo kot vsoto dveh kvadratov, npr. $2 = 1^2 + 1^2$, $5 = 2^2 + 1^2$, $17 = 4^2 + 1^2, \ldots$ V nadaljevanju si bomo ogledali katera števila lahko zapišemo kot vsoto dveh kvadratov, ter katera ne moremo zapisati kot vsoto dveh kvadratov. V dokazih bomo potrebovali nekaj pomožnih izrekov in sicer mali Fermatov izrek, ki pravi, da za praštevila p, ki ne delijo števila a velja, da $a^{p-1} \equiv 1 \pmod{p}$, Wilsonov izrek, da za praštevilo p velja $(p-1)! \equiv -1 \pmod{p}$, in izrek, da ima kvadratna kongruenca $x^2 + 1 \equiv 0 \pmod{p}$, kjer je p liho praštevilo, rešitev, če in samo če velja $p \equiv 1 \pmod{p}$. Vsi trije izreki so povzeti po [1].

Izrek 3.1. *(MALI FERMATOV IZREK) Če je p praštevilo in $p \nmid a$, potem je*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dokaz. Oglejmo si prvih $p-1$ večkratnikov števila a, to so števila

$$a,\ 2a,\ 3a, \ldots,\ (p-1)a.$$

Nobeni od teh števil nista med samo kongruentni po modulu p, niti ni nobeno kongruentno nič po modulu p. Sicer bi veljalo, da je

$$ra \equiv sa \pmod{p}, \quad 1 \leq r < s \leq p-1.$$

Torej lahko enačbo delimo z a (ker $p \nmid a$) in dobimo $r \equiv s \pmod{p}$, kar ni mogoče. Vemo, da so vsa ta števila a, $2a$, $3a, \ldots,$ $(p-1)a$ kongruentna 1, 2, $3, \ldots,$ $p-1$ po modulu p v nekem vrstnem redu. Torej, če med sabo pomnožimo te kongruence dobimo

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},$$

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Kongruenco lahko delimo s $(p-1)!$, saj $p \nmid (p-1)!$, ter dobimo

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Izrek 3.2. *(WILSONOV IZREK) Če je p praštevilo, potem velja*

$$(p-1)! \equiv -1 \pmod{p}.$$

Dokaz. Očitno izrek velja za $p = 2$ in $p = 3$. Torej predpostavimo, da je $p > 3$. Naj bo a eno izmed $p-1$ pozitivnih celih števil

$$1,\ 2,\ 3, \ldots,\ p-1,$$

ki zadošča linearni kongruenci $ax \equiv 1 \pmod{p}$. Potem velja $gcd(a,p) = 1$. Po izreku, da ima linearna kongruenca $ax \equiv b \pmod{n}$ rešitev, če in samo če $d|b$, kjer je $d = gcd(a,n)$. Če $d|b$, potem ima enačba d medsebojno nekongruentnih rešitev po modulu n. Torej v našem primeru ima enačba enolično rešitev po modulu p, torej enolično obstaja celo število a', tako da velja $1 \leq a' \leq p-1$ in zadošča kongruenci $aa' \equiv 1 \pmod{p}$.
Predpostavimo sedaj, da imamo v zgornji kongruenci $a = a'$. Najprej opazimo, da je kongruenca $a^2 \equiv 1 \pmod{p}$ ekvivalentna kongruenci $(a-1)(a+1) \equiv 0 \pmod{p}$. Torej je $a = a'$ lahko samo v primeru, ko je $a-1 \equiv 0 \pmod{p}$, ali ko je $a+1 \equiv 0 \pmod{p}$. V prvem primeru mora biti $a = 1$, medtem ko mora v drugem primeru veljati $a = p-1$. Torej v primeru $a = a'$ kongruenca $aa' \equiv 1 \pmod{p}$ velja natanko tedaj, ko je $a = 1$ ali $a = p-1$.
Če se vrnemo na množico števil $1,\ 2,\ 3, \ldots,\ p-1$ in izpustimo števili 1 ter $p-1$, ostala razvrstimo v pare a, a', tako da $a \neq a'$ in velja $aa' \equiv 1 \pmod{p}$. Dobimo $\frac{p-3}{2}$ parov števil ter kongruenc. Če vse kongruence zmnožimo ter člene uredimo po velikosti, dobimo

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$$

$$(p-2)! \equiv 1 \pmod{p}.$$

Kongruenco pomnožimo z $p-1$ ter dobimo

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p},$$

kar smo želeli dokazati. □

Izrek 3.3. *Kvadratna kongruenca $x^2 + 1 \equiv 0 \pmod{p}$, kjer je p liho praštevilo, ima rešitev, če in samo če velja $p \equiv 1 \pmod{4}$.*

Dokaz. ($\Rightarrow$) Naj bo a neka rešitev enačbe $x^2 + 1 \equiv 0 \pmod{p}$, torej velja $a^2 \equiv -1 \pmod{p}$. Ker velja $p \nmid a$, po Fermatovem izreku (Izrek 3.1) velja:

$$1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Recimo, da je p oblike $4k+3$, potem velja

$$(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1,$$

torej je $1 \equiv -1 \pmod{p}$. Iz tega sledi, da $p|2$, kar pa ne drži, saj je p liho praštevilo. Torej je p oblike $4k+1$.
($\Leftarrow$) Oglejmo si produkt

$$(p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2) \cdot (p-1)$$

ter naslednje kongrunece

$$\begin{aligned} p-1 &\equiv -1 \pmod{p}, \\ p-2 &\equiv -2 \pmod{p}, \\ &\vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod{p}. \end{aligned}$$

Od tod sledi

$$\begin{aligned} (p-1)! &\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \pmod{p} \\ &\equiv (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \pmod{p}. \end{aligned}$$

Če uporabimo Wilsonov izrek (Izrek 3.2) $(p-1)! \equiv -1 \pmod{p}$, potem dobimo

$$-1 \equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}.$$

Ker smo predpostavili, da je p oblike $4k+1$, sledi, da je $(-1)^{\frac{p-1}{2}} = 1$, torej velja

$$-1 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}.$$

Torej $\left(\frac{p-1}{2}\right)!$ zadošča kvadratni kongruenci $x^2 + 1 \equiv 0 \pmod{p}$, zato ima kvadratna kongruenca rešitev. □

Zelo uporabna je naslednja lema, ki pravi, da če lahko dve števili zapišemo kot vsoto dveh kvadratov, potem lahko tudi njun produkt zapišemo kot vsoto dveh kvadratov. Torej za generiranje števil, ki jih lahko zapišemo kot vsoto dveh kvadratov, je to zelo uporabna lema. V dokazu je tudi algoritem kako novo število, ki je produkt števil, zapišemo kot vsoto kvadratov.

Lema 3.4. [1] *Če lahko števili m in n vsako zapišemo kot vsoto dveh kvadartov, potem lahko tudi njun produkt mn zapišemo kot vsoto dveh kvadratov.*

Dokaz. Če sta $m = a^2 + b^2$ in $n = c^2 + d^2$ za cela števila a, b, c in d, potem je

$$mn = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2 = (ac + bd)^2 + (ad - bc)^2.$$

□

Primer 3.5. Naj bo $n = 17$ ter $m = 34$, torej lahko tudi število 578 zapišemo kot vsoto dveh kvadratov, saj je $17 = 4^2 + 1^2$ in $34 = 5^2 + 3^2$. Število $578 = (4 \cdot 5 + 1 \cdot 3)^2 + (4 \cdot 3 - 5 \cdot 1)^2 = 23^2 + 7^2$. ■

Izrek 3.6. [1] *Nobeno praštevilo p oblike $4k + 3$ ne moremo zapisati kot vsoto dveh kvadratov.*

Dokaz. Vsako celo število a je po modulu 4 kongruentno $0, 1, 2$ ali 3, od koder sledi, da je $a^2 \equiv 0$ ali $1 \pmod 4$. Torej za poljubni celi števili a in b velja

$$a^2 + b^2 \equiv 0, 1 \text{ ali } 2 \pmod 4.$$

Torej, če je $p \equiv 3 \pmod 4$, potem praštevila p ne moremo zapisati kot vsoto dveh kvadratov. □

Vsa ostala liha praštevila, ki so kongruentna 1 po modulu 4, pa lahko zapišemo kot vsoto dveh kvadratov. Dokaz le tega vsebuje izrek o kongruencah norveškega matematika Axela Thue, ki temelji na Dirikletovem principu ali načelu golobnjaka.

Izrek 3.7. [2] *(PRINCIP GOLOBNJAKA) Če n objektov razporedimo v m zabojev (ali golobe v kletke) in je $n > m$, potem vsaj en zaboj vsebuje več kot en objekt.*

Lema 3.8. [1] *(THUEVA LEMA) Naj bo p praštevilo in $gcd(a, p) = 1$. Potem ima kongruenca*

$$ax \equiv y \pmod p$$

rešitv x_0, y_0 za katero velja

$$0 < |x_0| < \sqrt{p} \text{ in } 0 < |y_0| < \sqrt{p}.$$

Dokaz. Naj bo $k = \lfloor \sqrt{p} \rfloor + 1$ in definirajmo množico števil

$$S = \{ax - y | 0 \leq x \leq k - 1, 0 \leq y \leq k - 1\}.$$

Izraz $ax - y$ zavzame $k^2 > p$ različnih vrednosti, zato po principu golobnjaka obstajata vsaj dve števili iz množice S, ki sta kongruentni po modulu p. Označimo ti dve števili z $ax_1 - y_1$ in $ax_2 - y_2$, kjer $x_1 \neq x_2$ ali $y_1 \neq y_2$. Torej velja:

$$ax_1 - y_1 \equiv ax_2 - y_2 \pmod p,$$

$$ax_1 - ax_2 \equiv y_1 - y_2 \ (mod\ p),$$

$$a(x_1 - x_2) \equiv y_1 - y_2 \ (mod\ p).$$

Označimo z $x_0 = x_1 - x_2$ ter z $y_0 = y_1 - y_2$, od koder sledi, da sta x_0 in y_0 rešitvi kongruence $ax \equiv y \ (mod\ p)$. Če bi kateri od x_0 ali y_0 bil enak nič, potem bi zaradi pogoja $gcd(a, p) = 1$ sledilo, da je tudi drugi enak nič, kar je v nasprotju s predpostavko. Torej je $0 < |x_0| \leq k - 1 < \sqrt{p}$ in $0 < |y_0| \leq k - 1 < \sqrt{p}$. □

S pomočjo do sedaj dokazanih izrekov in lem lahko dokažemo Fermatov izrek, ki pravi, da lahko vsako praštevilo oblike $4k + 1$ zapišemo kot vsoto dveh kvadratov. Fermat je svoje odkritje delil z Mersennom, kateremu je 25. decembra 1640 poslal pismo, v katerem je predstavil izrek ter trdil da ga je tudi dokazal. Kljub temu je dokaz tega izreka objavil Euler šele leta 1754, kateri je tudi dokazal, da je ta zapis enoličen. Povzeto po [1].

Izrek 3.9. *(FERMATOV IZREK) Liho praštevilo p lahko zapišemo kot vsoto dveh kvadratov, če in samo če velja, da je $p \equiv 1 \ (mod\ 4)$.*

Dokaz. ($\Rightarrow$) Recimo, da lahko p zapišemo kot vsoto dveh kvadratov, torej $p = a^2 + b^2$. Ker je p praštevilo sledi, da $p \nmid a$ in $p \nmid b$. (Ker je $p > a^2 \geq a$, praštevilo p sigurno ne deli a. Podobno vidimo, da p ne deli b.) Po pravilih o linearnih kongruencah (theory of linear congruences) obstaja celo število c, tako da velja

$$bc \equiv 1 \ (mod\ p). \tag{3.1}$$

Če enačbo $a^2 + b^2 = p$ pomnožimo s c^2 dobimo

$$(ac)^2 + (bc)^2 = pc^2. \tag{3.2}$$

Torej iz (3.1) in (3.2) sledi

$$(ac)^2 \equiv -1 \ (mod\ p),$$

kar pomeni, da je -1 kvadratni ostanek od p. Po Posledici 2.10 sledi $\left(\frac{-1}{p}\right) = 1$, kar velja samo v primeru, da je $p \equiv 1 \ (mod\ 4)$.
($\Leftarrow$) Recimo, da je $p \equiv 1 \ (mod\ 4)$. Torej je -1 kvadratni ostanek od p, zato po Izreku 3.3 obstaja celo število a, tako da $a^2 \equiv -1 \ (mod\ p)$, $a = \left(\frac{(p-1)}{2}\right)!$. Ker je $gcd(a, p) = 1$ ima kongruenca

$$ax \equiv y \ (mod\ p)$$

rešitev x_0, y_0, za katero velja pogoj iz Leme 3.8. Iz tega izpeljemo

$$-x_0^2 \equiv a^2 x_0^2 \equiv (ax_0)^2 \equiv y_0^2 \ (mod\ p),$$

$$x_0^2 + y_0^2 \equiv 0 \ (mod\ p).$$

To pomeni, da je

$$x_0^2 + y_0^2 = kp \tag{3.3}$$

za nako celo število $k > 0$. Ker po Lemi 3.8 velja $0 < |x_0| < \sqrt{p}$ in $0 < |y_0| < \sqrt{p}$, sledi, da je

$$0 < x_0^2 + y_0^2 < 2p. \tag{3.4}$$

Torej po (3.3) in (3.4) sledi, da je $kp < 2p$, torej je $k = 1$ in zato velja $x_0^2 + y_0^2 = p$. □

Posledica 3.10. *Vsako praštevilo p oblike $4k + 1$ lahko enolično predstavimo (do vrstnega reda členov natančno) kot vsoto dveh kvadratov.*

Dokaz. Recimo, da velja

$$p = a^2 + b^2 = c^2 + d^2,$$

kjer so a, b, c, d pozitivna cela števila. Potem velja

$$a^2d^2 - b^2c^2 = p(d^2 - b^2) \equiv 0 \ \ (mod \ \ p) \tag{3.5}$$

od koder sledi, da je $ad \equiv bc \ \ (mod \ \ p)$ ali $ad \equiv -bc \ \ (mod \ \ p)$. Ker so a, b, c, d vsi manjši od $\sqrt{p}$ iz (3.5) sledi, da je

$$ad - bc = 0$$

ali

$$ad + bc = p. \tag{3.6}$$

Če velja pogoj (3.6), potem sledi

$$p^2 = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$$

$$= a^2d^2 + 2abcd + b^2c^2 + a^2c^2 - 2abcd + b^2d^2 = (ad + bc)^2 + (ac - bd)^2 =$$

$$= p^2 + (ac - bd)^2,$$

torej je $ac - bd = 0$. Od tod sledi, da velja

$$ad = bc \quad \text{ali} \quad ac = bd.$$

Poglejmo najprej primer, ko je $ad = bc$. Potem $a|bc$ in ker je $gcd(a, b) = 1$, sledi, da $a|c$. Torej je $c = ka$, za neko celo število k. Iz pogoja $ad = bc = b(ka)$ sledi, da je $d = bk$. Ampak

$$p = c^2 + d^2 = k^2(a^2 + b^2),$$

torej je $k = 1$.V tem primeru iz $c = ka$ sledi, da je $a = c$, potem pa iz $ad = bc$ sledi tudi, da je $b = c$. S podobnimi argumenti pridemo do enakega zaključka tudi v primeru, ko je $ac = bd$. Torej smo s tem dokazali enoličnost. □

Primer 3.11. Oglejmo si prvih nekaj lihih praštevil, ki dajo ostanek 1 pri deljenju s 4.

$$5 = 2^2 + 1^2,$$

$$13 = 3^2 + 2^2,$$

$$17 = 4^2 + 1^2,$$

$$29 = 5^2 + 2^2,$$

$$37 = 6^2 + 1^2,$$

$$41 = 5^2 + 4^2,$$

$$\vdots$$

■

Primer 3.12. [1] Oglejmo si kako praštevilo $p = 13$ zapišemo kot vsoto dveh kvadratov, če sledimo dokazu Fermatovega izreka (Izrek 3.9). Potem je $a = \left(\frac{p-1}{2}\right)! = 6! = 720$. Torej iščemo rešitve kongruence

$$720x \equiv y \pmod{13},$$

katera je evivalentna kongruenci

$$5x \equiv y \pmod{13}. \tag{3.7}$$

Definirajmo množico

$$S = \{5x - y | 0 \leq x, y < 4\}.$$

Torej elementi množice S so števila

$$\begin{array}{cccc} 0 & 5 & 10 & 15 \\ -1 & 4 & 9 & 14 \\ -2 & 3 & 8 & 13 \\ -3 & 2 & 7 & 12, \end{array}$$

ki so po modulu 13 enaka:

$$\begin{array}{cccc} 0 & 5 & 10 & 2 \\ 12 & 4 & 9 & 1 \\ 11 & 3 & 8 & 0 \\ 10 & 2 & 7 & 12. \end{array}$$

Sedaj imamo veliko možnosti za izbiro x in y, ki ustrezata kongruenci (3.7). Recimo da izberemo

$$5 \cdot 1 - 3 \equiv 2 \equiv 5 \cdot 3 - 0 \pmod{13}$$

oziroma

$$5(1-3) \equiv 3 \pmod{13}.$$

Torej rešitvi sta $x_0 = -2$ in $y_0 = 3$. Torej lahko 13 zapišemo kot vsoto dveh kvadratov na sldeč način:

$$13 = x_0^2 + y_0^2 = 2^2 + 3^2.$$

■

Do sedaj smo se posvečali samo praštevilom, katere lahko oziroma ne moremo zapisati kot vsote dveh kvadratov. Sedaj poglejmo še ostala števila. Ključnega pomena so prafaktorji oblike $4k+3$. Naravno število oblike N^2m, kjer je m kvadratov prosto število, lahko zapišemo kot vsoto dveh kvadratov, če in samo če m ne vsebuje prafaktorja oblike $4k+3$. Povedano z drugimi besedami, naravno število lahko zapišemo kot vsoto dveh kvadratov, če in samo če je vsak njegov prafaktor oblike $4k+3$ na sodo potenco.

Izrek 3.13. [1] *Naj bo n naravno število oblike $n = N^2m$, kjer je m kvadratov prosto število. Potem lahko n zapišemo kot vsoto dveh kvadratov, če in samo če m ne vsebuje prafaktorjev oblike $4k+3$.*

Dokaz. ($\Leftarrow$) Predpostavimo, da m nima prafaktorjev oblike $4k+3$. Če je $m = 1$, potem je $n = N^2 + 0^2$. Če pa je $m > 1$, potem ga lahko zapišemo kot $m = p_1p_2 \cdots p_r$, kjer so p_r med sabo različna praštevila. Vsako izmed njih je enako 2 ali pa je oblike $4k+1$. Torej lahko vsako od teh praštevil po Izreku 3.9 zapišemo kot vsoto dveh kvadratov. Torej obstajata taki števili x in y, da je $m = x^2 + y^2$. Prav tako pa po Lemi 3.4 velja, da lahko produkt dveh števil, ki jih lahko zapišemo kot vsoto dveh kvadratov, zapišemo kot vsoto dveh kvadratov. Torej velja

$$n = N^2m = N^2(x^2 + y^2) = (Nx)^2 + (Ny)^2.$$

($\Rightarrow$) Dokažimo še obratno smer. Predpostavimo, da lahko n zapišemo kot vsoto dveh kvadratov

$$n = a^2 + b^2 = N^2m$$

in naj bo p nek praštevilski deljitelj števila m. Brez škode za splošnost lahko predpostavimo, da je $m > 1$. Naj bo $d = gcd(a, b)$, potem je $a = rd$ in $b = sd$, pri čemer sta r in s tuji si števili. Iz tega sledi

$$d^2(r^2 + s^2) = N^2m.$$

Zato ker je m kvadratov prosto število sledi, da $d^2|N^2$, ampak potem velja

$$r^2 + s^2 = \left(\frac{N^2}{d^2}\right) m = tp$$

za neko celo število t, kar nas pripelje do kongruence

$$r^2 + s^2 \equiv 0 \ (mod \ p). \tag{3.8}$$

Iz pogoja $gcd(r, s) = 1$ sledi, da je eden izmed r ali s, recimo da r, tuj številu p. Zato obstaja število r', ki zadošča kongruneci

$$rr' \equiv 1 \ (mod \ p). \tag{3.9}$$

Če enačbo (3.8) pomnožimo z $(r')^2$ ter upoštevamo (3.9), dobimo

$$(sr')^2 + 1 \equiv 0 \ (mod \ p),$$

kar pomeni, da je -1 kvadratni ostanek po modulu p, zato je Legendrov simbol $\left(\frac{-1}{p}\right) = 1$. Po Izreku 3.9 sledi, da je $p \equiv 1 \ (mod \ p)$. Torej noben delitelj števila m ni oblike $4k + 3$. □

Primer 3.14. Oglejmo si uporabo Izreka 3.13 na dveh primerih.

- Najprej število $605 = 11^2 \cdot 5$, katero je oblike N^2m in za m velja da je oblike $4k + 1$, saj je $5 = 4 \cdot 1 + 1$.Vemo, da je $5 = 2^2 + 1^2$, torej velja

$$605 = 11^2 \cdot 5 = 11^2(2^2 + 1^2) = 22^2 + 11^2 = 484 + 121 = 605.$$

- Poglejmo še malo večje število $1360 = 4^2 \cdot 5 \cdot 17$, kjer je $N = 4$ ter $m = 5 \cdot 17 = 85$, torej noben delitelj števila m ni oblike $4k + 3$. V tem primeru bomo poleg Izreka 3.13 uporabili tudi Lemo 3.4.

$$1360 = 4^2 \cdot 5 \cdot 17 = 4^2(2^2 + 1^2)(4^2 + 1^2) = 4^2((2 \cdot 4 + 1 \cdot 1)^2 + (2 \cdot 1 - 1 \cdot 4)^2) =$$

$$= 4^2(9^2 + (-2)^2) = 36^2 + (-8)^2 = 36^2 + 8^2 = 1296 + 64 = 1360.$$

■

Primer 3.15. Samo za števila oblike $4k + 1$ velja enoličnost zapisa kot vsoto dveh kvadratov. Recimo število $50 = 5^2 \cdot 2$ ni oblike $4k + 1$, vendar ustreza pogojem Izreka 3.13, zato ga lahko zapišemo kot vsoto dveh kvadratov. Posebnost je, da ga lahko zapišemo na dva različna načina kot vsoto dveh kvadratov.

$$50 = 5^2 + 5^2 = 7^2 + 1^2.$$

■

Posledica 3.16. [1] *Naravno število n lahko zapišemo kot vsoto dveh kvadratov, če in samo če je vsak prafaktor oblike* $4k + 3$ *na sodo potenco.*

Če lahko število zapišemo kot vsoto dveh kvadratov, zakaj ga ne bi mogli zapisati tudi kot razliko dveh kvadratov? Izkaže se, da lahko število zapišemo kot razliko dveh kvadratov, če število ni oblike $4k + 2$. Še bolj zanimiva pa so liha praštevila. Zanje velja, da jih lahko zapišemo kot razliko kvadratov dveh zaporednih naravnih števil. Ta izrek in posledica sta povzeta po [1].

Izrek 3.17. *Pozitivno celo število n lahko zapišemo kot razliko dveh kvadratov, če in samo če n ni oblike $4k + 2$.*

Dokaz. Za vsako naravno število a velja, da je $a^2 \equiv 0$ *ali* $1 \pmod 4$. Od tod sledi, da je

$$a^2 - b^2 \equiv 0,\ 1 \text{ ali } 3 \pmod 4.$$

Torej, če je $n \equiv 2 \pmod 4$, potem ga ne moremo zapisati kot $n = a^2 - b^2$ za nobeni števili a in b.
Poglejmo na kakšen način lahko števila zapišemo kot razliko dveh kvadratov. Recimo, da n ni oblike $4k+2$, torej je $n \equiv 0, 1$ *ali* $3 \pmod 4$. Če je $n \equiv 1$ *ali* $3 \pmod 4$, potem sta $n + 1$ in $n - 1$ obe sodi števili, zato lahko n zapišemo kot razliko dveh kvadratov takole:

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2.$$

Če je $n \equiv 0 \pmod 4$, potem velja

$$n = \left(\frac{n}{4} + 1\right)^2 - \left(\frac{n}{4} - 1\right)^2.$$

□

Primer 3.18. Oglejmo si primer $n = 117$. Ker ni oblike $4k + 2$ ga lahko zapišemo kot razliko dveh kvadratov.

$$117 = 13 \cdot 3^2$$

Kot razliko kvadratov ga lahko zapišemo na dva različna načina

$$117 = 13 \cdot 9 = \left(\frac{13+9}{2}\right)^2 - \left(\frac{13-9}{2}\right)^2 = 11^2 - 2^2$$

$$117 = 39 \cdot 3 = \left(\frac{39+3}{2}\right)^2 - \left(\frac{39-3}{2}\right)^2 = 21^2 - 18^2$$

Posledica 3.19. *Liho praštevilo lahko zapišemo kot razliko kvadratov dveh zaporednih naravnih števil.*

Dokaz. Naj bo p praštevilo, ki ga lahko zapišemo kot razliko kvadratov

$$p = a^2 - b^2 = (a - b)(a + b),$$

kjer je $a > b > 0$. Ker je p praštevilo, sta 1 in p edina deljitelja, zato sledi

$$a - b = 1 \ in \ a + b = p,$$

od koder sledi

$$a = \frac{p+1}{2} \ in \ b = \frac{p-1}{2}.$$

Torej, liho praštevilo p lahko zapišemo kot razliko kvadratov dveh zapirednih naravnih števil. Zapis je enoličen in je enak

$$p = \left(\frac{p+1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2.$$

□

Oglejmo si nekaj lihih praštevil, ter jih zapišimo kot razliko kvadratov dveh zaporednih naravnih števil.

Primer 3.20.

$$11 = 6^2 - 5^5,$$

$$13 = 7^2 - 6^2,$$

$$17 = 9^2 - 8^2,$$

$$19 = 10^2 - 9^2.$$

■

4 PREDSTAVITEV NARAVNIH ŠTEVIL KOT VSOTE TREH KVADRATOV

Katera števila lahko zapišemo kot vsoto dveh kvadratov, katera kot vsoto treh kvadratov in katera kot vstoto štirih kvadratov? Najtežje vprašanje izmed teh je sigurno katera števila lahko zapišemo kot vsoto treh kvadratov. Kar trideset let za dokazom, da lahko vsako število zapišemo kot vsoto štirih kvadratov, je Legendru uspelo ugotoviti ter dokazati, da lahko število zapišemo kot vsoto treh kvadratov, če in samo če ni oblike $4^x(8y+7)$, kjer sta x in y nenegativni celi števili. Za sam dokaz bomo potrebovali kar nekaj pomožnih izrekov, lem ter definicij. Najprej si oglejmo dve lemi, ki vključujeta kongrunece po modulu 8, ki sta povzeti po [3].

Lema 4.1. *Kvadrat naravnega števila je kongruenten* $0, 1$ *ali* 4 *po modulu* 8.

Dokaz. Obravnavajmo vse možnosti. Naravno število n je kongruentno $0, 1, 2, 3, 4, 5, 6$ ali 7 po modulu 8.

$$n \equiv 0 \pmod 8 \Rightarrow n^2 \equiv 0 \pmod 8,$$

$$n \equiv 1 \pmod 8 \Rightarrow n^2 \equiv 1 \pmod 8,$$

$$n \equiv 2 \pmod 8 \Rightarrow n^2 \equiv 4 \pmod 8,$$

$$n \equiv 3 \pmod 8 \Rightarrow n^2 \equiv 1 \pmod 8,$$

$$n \equiv 4 \pmod 8 \Rightarrow n^2 \equiv 0 \pmod 8,$$

$$n \equiv 5 \pmod 8 \Rightarrow n^2 \equiv 1 \pmod 8,$$

$$n \equiv 6 \pmod 8 \Rightarrow n^2 \equiv 4 \pmod 8,$$

$$n \equiv 7 \pmod 8 \Rightarrow n^2 \equiv 1 \pmod 8.$$

Torej kvadrat naravnega števila je kongruenten po modulu 8 samo vrednostim $0, 1$ ali 4. □

Lema 4.2. *Ne obstaja množica treh celih števil* $\{a, b, c\}$*, tako da je* $a^2 + b^2 + c^2 \equiv 7 \pmod 8$.

Dokaz. Po Lemi 4.1 vemo, da je kvadrat naravnega števila n kongruenten po modulu 8 le številom $0, 1$ ali 4. Torej oglejmo si vse možne kombinacije za vsoto treh kvadratov.

$$0+0+0=0\equiv 0 \ (mod\ 8),$$

$$1+0+0=1\equiv 1 \ (mod\ 8),$$

$$1+1+0=2\equiv 2 \ (mod\ 8),$$

$$1+1+1=3\equiv 3 \ (mod\ 8),$$

$$4+0+0=4\equiv 4 \ (mod\ 8),$$

$$4+4+0=8\equiv 0 \ (mod\ 8),$$

$$4+4+4=12\equiv 4 \ (mod\ 8),$$

$$1+4+0=5\equiv 5 \ (mod\ 8),$$

$$1+1+4=6\equiv 6 \ (mod\ 8),$$

$$1+4+4=9\equiv 1 \ (mod\ 8).$$

Torej vsota treh kvadratov ni nikoli kongruentna 7 po modulu 8. □

V dokazu bomo potrebovali znanje o kvadratnih formah v treh spremenljivkah. Oglejmo si definicijo ter nekaj lastnosti, ki so povzete po [3].

Definicija 4.3. Celoštevilska kvadratna forma v treh spremenljivkah je preslikava F iz $\mathbb{R}^3$ v $\mathbb{R}$, definirana takole

$$F(x,y,z)=a_{11}x^2+2a_{12}xy+2a_{13}xz+a_{22}y^2+2a_{23}yz+a_{33}z^2,$$

kjer so $a_{11},\ a_{12},\ a_{13},\ a_{22},\ a_{23},\ a_{33}$ poljubna cela števila. Celoštevilska kvadratna forma v treh spremenljivkah je pozitivno-definitna, če je $F(x,y,z)\geq 0$ za poljubna cela števila $x,\ y,\ z$, in je $F(x,y,z)=0$, če in samo če je $x=y=z=0$.

Definicija 4.4. Determinanta celoštevilske kvadratne forme v treh spremenljivkah je determinanta matrike

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{bmatrix},$$

kjer so $a_{11},\ a_{12},\ a_{13},\ a_{22},\ a_{23},\ a_{33}$ koeficienti forme. Determinanto celoštevilske kvadratne forme označimo $det(F)$.

Definicija 4.5. Naj bo F celoštevilska kvadratna forma v treh spremenljivkah in naj bo n poljubno naravno število. Rečemo, da forma F reprezentira število n, če obstajajo taka cela števila $x_0,\ y_0,\ z_0$, da je $n=F(x_0,y_0,z_0)$.

Izrek 4.6. *Naj bo* $F(x,y,z) = a_{11}x^2 + 2a_{12}xy + 2a_{13}xz + a_{22}y^2 + 2a_{23}yz + a_{33}z^2$ *celoštevilska kvadratna forma v treh spremenljivkah. Potem je forma* $F(x,y,z)$ *pozitivno-definitna, če in samo če je* $a_{11} > 0$, $a_{11}a_{22} - a_{12}^2 > 0$ *in je* $det(F) > 0$.

Izrek 4.7. *Naj bo* $F(x,y,z)$ *celoštevilska pozitivno-definitna kvadratna forma v treh spremenljivkah, ki ima determinanato* 1. *Če forma* F *reprezentira naravno število* n *(torej, če za neka cela števila* x_0, y_0, z_0 *velja, da je* $F(x_0,y_0,z_0) = n$*), potem obstajajo taka cela števila* m_1, m_2, m_3, *da je* $n = m_1^2 + m_2^2 + m_3^2$.

Oglejmo si nekaj novih pojmov in sicer red števila, primitivni koren ter definicijo Eulerjeve funkcije. Te pojme bomo uporabili v nadaljnih pomožnih izrekih ter posledici potrebnih za dokaz glavnega izreka, katera števila lahko oziroma ne moremo zapisati kot vsoto treh kvadratov. Pomožna izreka sta Eulerjev kriterij, ki pravi, da je a kvadratni ostanek od p natanko tedaj, ko je $a^{\frac{p-1}{2}} \equiv 1 \pmod{n}$ ter da velja $a^h \equiv 1 \pmod{p}$, če in samo če $k|h$, kjer je a celo število z redom k po modulu n. Definicija in izreki so povzeti po [1].

Definicija 4.8. Naj bo $n > 1$ in $gcd(a,n) = 1$. Red števila a po modulu n je najmanjše naravno število k, ki zadošča $a^k \equiv 1 \pmod{n}$.

Definicija 4.9. Za vsak $n \geq 1$, naj $\phi(n)$ označuje število naravnih števil, ki so manjša ali enaka n in so tuja številu n. Funkcijo $\phi(n)$ imenujemo Eulerjeva funkcija.

Definicija 4.10. Če je $gcd(a,n) = 1$ in je a reda $\phi(n)$ po modulu n, potem je a primitivni koren od n.

Izrek 4.11. *Naj bo* a *celo število z redom* k *po modulu* n. *Potem je* $a^h \equiv 1 \pmod{n}$, *če in samo če* $k|h$.

Dokaz. ($\Leftarrow$) Recimo, da $k|h$, potem velja $h = kj$ za neko celo število j. Ker velja $a^k \equiv 1 \pmod{n}$, sledi, da je $(a^k)^j \equiv 1^j \pmod{n}$. Torej je $a^h \equiv 1 \pmod{n}$.
($\Rightarrow$) Recimo, da je h tako pozitivno število, ki zadošča $a^h \equiv 1 \pmod{n}$. Po izreku o deljenju obstajata taki števili q in r, da velja $h = qk + r$, kjer je $0 \leq r < k$. Iz tega sledi

$$a^h = a^{qk+r} = (a^k)^q a^r.$$

Po predpostavki velja $a^h \equiv 1 \pmod{n}$ in $a^k \equiv 1 \pmod{n}$, zato sledi $a^r \equiv 1 \pmod{n}$. Ker je $0 \leq r < k$, sledi, da je $r = 0$. Če je namreč $r > 0$, potem pridemo v protisovje z minimalnostjo števila k. Zato velja $h = qk$, torej $k|h$. □

Izrek 4.12. *(EULERJEV KRITERIJ) Naj bo* p *liho praštevilo in* $gcd(a,p) = 1$. *Potem je* a *kvadratni ostanek od* p, *če in samo če velja* $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Dokaz. ($\Rightarrow$) Denimo, da je a kvadratni ostanek od p. Torej ima kongruenca $x^2 \equiv a \pmod{p}$ rešitev. Rešitev te kongruence označimo z x_1. Ker velja $gcd(a,p) = 1$, sledi, da je tudi $gcd(x_1, p) = 1$. Oglejmo si vrednost števila $a^{\frac{p-1}{2}}$ po modulu p :

$$a^{\frac{p-1}{2}} \equiv (x_1^2)^{\frac{p-1}{2}} \equiv x_1^{p-1} \pmod{p}.$$

Ob upoštevanju malega Fermatovega izreka (Izrek 3.1) sledi

$$a^{\frac{p-1}{2}} \equiv x_1^{p-1} \equiv 1 \pmod{p}.$$

($\Leftarrow$) Recimo, da je $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ in naj bo r primitivni koren od p. Potem velja $a \equiv r^k \pmod{p}$ za neko celo število k, $1 \leq k \leq p-1$. Torej velja

$$r^{\frac{k(p-1)}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Ker je r primitivni koren praštevila p, je njegov red $\phi(p) = p-1$. Po Izreku 4.11 mora red r deliti eksponent $\frac{k(p-1)}{2}$. Torej je k sodo število in ga zapišimo kot $k = 2j$. Sledi

$$(r^j)^2 = r^{2j} = r^k \equiv a \pmod{p},$$

kar pomeni, da je r^j rešitev kongruence $x^2 \equiv a \pmod{p}$. To pomeni, da je a kvadratni ostanek praštevila p. □

Če je p liho praštevilo in velja $gcd(a,p) = 1$, potem je

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = a^{p-1} - 1 \equiv 0 \pmod{p},$$

zaradi upoštevanja malega Fermatovega izreka (Izrek 3.1). Torej velja

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad ali \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

vendar ne oboje hkrati. Saj, če bi veljalo oboje hkrati, bi sledilo, da je $1 \equiv -1 \pmod{p}$, kar pomeni, da $p|2$, kar je pa v nasprotju s pogojem, da je p liho praštevilo. Torej, ker kvadratni neostanek ne ustreza $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, mora ustrezati $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. To nas pripelje do naslednje posledice.

Posledica 4.13. [1] *Naj bo p liho praštevilo in $gcd(a,p) = 1$. Potem je a kvadratni ostanek praštevila p natanko tedaj, ko je*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Podobno, a je kvadratni neostanek praštevila p natanko tedaj, ko je

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Sledi Dirichletov izrek o aritmetičnem zaporedju.

Izrek 4.14. [3] *(DIRICHLETOV IZREK O ARITMETČNEM ZAPOREDJU) Naj bosta q in m celi števili, za kateri velja $gcd(q, m) = 1$. Potem obstaja neskončno mnogo praštevil, ki so kongruentne q po modulu m. To pomeni, da aritmetično zporednje q, $q+m$, $q+2m$, $q+3m, \ldots$ vsebuje neskončno mnogo praštevil.*

Dokaz. Dokaz si lahko prebrete v [6].

Glavni rezultat tega poglavja je naslednji izrek, da lahko število zapišemo kot vsoto treh kvadratov, če in samo če ni oblike $4^x(8y + 7)$, kjer sta x in y nenegativni celi števili. Obstaja več različnih dokazov za ta izrek. Za potreben pogoj izreka smo izbrali Dirichletov klasičen dokaz. Dokaz je povzet po [3].

Izrek 4.15. *Naravno število n je oblike $n = 4^x(8y+7)$, kjer sta x in y nenegativni celi števili, če in smo če ga ne moremo zapisati kot vsoto treh kvadratov.*

Dokaz. ($\Rightarrow$) Predpostavimo, da je n naravno število oblike $4^x(8y + 7)$. Če je $x \geq 1$, potem je $n \equiv 0 \pmod 4$.
Ta del dokaza bomo dokazali s protislovjem. Torej predpostavimo, da obstajajo cela števila p, q, r, tako da je $p^2 + q^2 + r^2 = n$. Če je n deljiv s 4, morajo biti p, q in r soda števila. Torej sledi

$$\frac{n}{4} = \left(\frac{p}{2}\right)^2 + \left(\frac{q}{2}\right)^2 + \left(\frac{r}{2}\right)^2 = 4^{x-1}(8y + 7).$$

Ta postopek ponovimo x krat. Torej obstajajo cela števila a, b, c, da je $a^2 + b^2 + c^2 = 8y + 7$, kar je v nasprotju z Lemo 4.2.

($\Leftarrow$) Dokazati moramo, da če n ne moremo zapisati kot vsoto treh kvadratov, potem je oblike $4^x(8y + 7)$, kar je ekvivalentno, da če n ni oblike $4^x(8y + 7)$, potem ga lahko zapišemo kot vsoto treh kvadratov.
Najprej opazimo, da je dovolj izrek dokazati za takšna števila n, ki niso deljiva s 4. Namreč, če je n deljiv s 4, potem ga lahko zapišemo v obliki $n = 4^x n_1$, kjer je x naravno število, n_1 pa naravno število, ki ni deljivo s 4. Če je sedaj $n_1 = a^2 + b^2 + c^2$ za neka cela števila a, b, c, potem je

$$n = 4^x n_1 = 4^x(a^2 + b^2 + c^2) = 2^{2x}(a^2 + b^2 + c^2) = (2^x a)^2 + (2^x b)^2 + (2^x c)^2.$$

Torej predpostavimo, da n ni oblike $4^x(8y+7)$ in da ni deljiv s 4. Torej je n liho število ali dvakratnik lihega števila, tako da velja $n \not\equiv 7 \pmod 8$. Torej, ker $n \not\equiv 0 \pmod 4$, velja $n \equiv 1, 2, 3, 5, 6 \pmod 8$. Po Izreku 4.7 vemo, da če obstaja pozitivno-definitna

kvadratna forma $F(x, y, z)$ z determinanto 1, ki reprezentira število n, potem lahko število n zapišemo kot vsoto treh kvadratov. Če želimo, da je F celoštevilska pozitivno-definitna kvadratna forma v treh spremenljivkah, ki reprezentira število n, potem mora po Izreku 4.6 zadoščati naslednjim pogojem

$$(a) = \begin{cases} F(x,y,z) = a_{11}x^2 + 2a_{12}xy + 2a_{13}xz + a_{22}y^2 + 2a_{23}yz + a_{33}z^2, \text{ za neka cela} \\ \qquad\qquad \text{števila } a_{11},\ a_{12},\ a_{13},\ a_{22},\ a_{23},\ a_{33}, \\ \text{obstajajo taka cela števila } x_0,\ y_0,\ z_0, \text{ da je } n = F(x_0, y_0, z_0), \\ a_{11} > 0, \\ a_{11}a_{22} - a_{12}^2 > 0, \\ det(F) = 1. \end{cases}$$

Še več, prepostavimo lahko, da velja

$$a_{13} = 1,\ \ a_{23} = 0,\ \ a_{33} = n,\ \ x_0 = 0,\ \ y_0 = 0,\ \ z_0 = 1. \tag{4.1}$$

Kasneje bomo namreč dokazali, da obstaja kvadratna forma, ki zadošča tako pogojem (a) kot pogojem (4.1). Označimo število $a_{11}a_{22} - a_{12}^2$ z b. Če upoštevamo, da je $a_{13} = 1$, $a_{23} = 0$ in $a_{33} = n$, potem dobimo, da je $det(F) = nb - a_{22}$. Ker je $det(F) = 1$, je torej $a_{22} = bn - 1$, in se zato pogoj (a) z upoštevanjem pogojev (4.1) preoblikuje v naslednje pogoje:

$$(b) = \begin{cases} a_{11} > 0, \\ b = a_{11}a_{22} - a_{12}^2 > 0, \\ a_{22} = bn - 1. \end{cases}$$

Če je $n = 1$, potem seveda trivialno sledi, da je $n = 0^2 + 0^2 + 1^2$. Torej od sedaj naprej privzemimo, da je $n > 1$. Ker sta b in n celi števili večji od 0 in je $n \geq 2$, sledi, da je $a_{22} = bn - 1 > b - 1 \geq 0$. Pravtako velja, da je $a_{12}^2 \geq 0$, zato je $a_{11}a_{22} = a_{12}^2 + b > 0$. Sledi, da mora biti $a_{11} > 0$. Torej lahko poenostavimo pogoj (b) in dobimo

$$(c) = \begin{cases} b = a_{11}a_{22} - a_{12}^2 > 0, \\ a_{22} = bn - 1. \end{cases}$$

Opazimo, da velja $(a) \iff (b) \iff (c)$. Torej moramo poiskati cela števila b, a_{11}, a_{22}, a_{12}, ki ustrezajo pogojem (c). Ker je $b > 0$, velja $-b \equiv a_{12}^2\ (mod\ bn - 1)$, torej mora biti $-b$ kvadratni ostanek po modulu $bn-1$. Dokaz razdelimo na dva primera.

Prvi primer: naj bo $n \equiv 2$ *ali* $6\ (mod\ 8)$.

Z Evklidovim algoritmom izračunamo največji skupni deljitelj števil $4n$ in $n-1$.

$n = 8k+2$:	$n = 8k+6$:
$4n = 32k+8, n-1 = 8k+1$	$4n = 32k+24, n-1 = 8k+5$
Evklidov algoritem za 4n in n-1	*Evklidov algoritem za 4n in n-1*
$32k+8 = 4(8k+1)+4$	$32k+24 = 4(8k+5)+4$
$8k+1 = 2k \cdot 4+1$	$8k+5 = (2k+1) \cdot 4+1$
$4 = 4 \cdot 1+0$	$4 = 4 \cdot 1+0$

V obeh primerih velja $gcd(4n, n-1) = 1$. Torej po Dirichletovem izreku o aritmetičnem zaporedju (Izrek 4.14) obstaja praštevilo p, ki zadošča kongruenci $p \equiv n-1 \pmod{4n}$. Iz tega sledi, da je

$$p = 4nk + n - 1 = (4k+1)n - 1$$

za neko naravno število k. Naj bo $b = 4k+1$. Potem je $b > 0$ in $p = bn - 1$. Ker je $b \equiv 1 \pmod 4$ po Jacobijevih zakonih velja

$$\begin{aligned}
\left(\frac{-b}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{b}{p}\right) \text{ po točki (2.9) Izreka 2.25} \\
&= \left(\frac{b}{p}\right) \text{ po Izreku 2.27 in ker je } \frac{p-1}{2} \text{ sodo število} \\
&= \left(\frac{p}{b}\right) \text{ po Izreku 2.26 ker je } \frac{p-1}{2} \text{ sodo število} \\
&= \left(\frac{bn-1}{b}\right), \text{ saj je p=bn-1} \\
&= \left(\frac{-1}{b}\right) \text{ po Lemi 2.24} \\
&= (-1)^{\frac{b-1}{2}} \text{ po Izreku 2.27} \\
&= 1, \text{ saj je b=4k+1 in je zato } \frac{b-1}{2} = 2k.
\end{aligned}$$

Torej je $-b$ kvadratni ostanek po modulu $p = bn - 1$. Zaradi tega je kongruenca $x^2 \equiv -b \pmod p$ rešljiva. Naj bo koeficient a_{12} ena od rešitev te kongruence. Torej je a_{12} celo število. Koeficient $a_{22} = bn - 1$, je pravtako celo število, saj sta b in n celi števili. Za koeficient a_{11} pa velja

$$a_{11} = \frac{b + a_{12}^2}{a_{22}} = \frac{b + a_{12}^2}{bn-1} = \frac{b + a_{12}^2}{p}.$$

Iz kongruence $a_{12}^2 \equiv -b \pmod p$ sledi, da $p | a_{12}^2 + b$, torej je tudi a_{11} celo število.

Drugi primer: naj bo $n \equiv 1,\ 3$ *ali* $5 \pmod 8$.
Z Evklidovim algoritmom izračunamo največji skupni deljitelj števil $4n$ ter $\frac{cn-1}{2}$, kjer

je $c = 1$, če je $n \equiv 3 \pmod 8$ in $c = 3$, če je $n \equiv 1 \ ali \ 5 \pmod 8$.) Evklidov algoritem za 4n in $\frac{cn-1}{2}$:

$n = 8k + 3 :$	$n = 8k + 1 :$
$4n = 32k + 12$	$4n = 32k + 4$
$\frac{cn-1}{2} = 4k + 1$	$\frac{cn-1}{2} = 12k + 1$
$32k + 12 = 8(4k + 1) + 4$	$32k + 4 = 2(12k + 1) + 8k + 2$
$4k + 1 = k \cdot 4 + 1$	$12k + 1 = 1(8k + 2) + 4k - 1$
$4 = 4 \cdot 1 + 0$	$8k + 2 = 2(4k - 1) + 4$
	$4k + 1 = k \cdot 4 + 1$
	$4 = 4 \cdot 1 + 0$

$$
\begin{aligned}
&n = 8k + 5 :\\
&4n = 32k + 20\\
&\tfrac{cn-1}{2} = 12k + 7\\
&\\
&32k + 20 = 2(12k + 7) + 8k + 6\\
&12k + 7 = 1(8k + 6) + 4k + 1\\
&8k + 6 = 2(4k + 1) + 4\\
&4k + 1 = k \cdot 4 + 1\\
&4 = 4 \cdot 1 + 0
\end{aligned}
$$

Torej največji skupni deljitelj je $gcd(4n, \frac{cn-1}{2}) = 1$. Po Dirichletovem izreku o aritmetičnem zaporedju (Izrek 4.14) obstaja praštevilo p, ki zadošča kongruenci $p \equiv \frac{cn-1}{2} \pmod{4n}$, zato velja, da je

$$p = 4nk + \frac{cn - 1}{2} = \frac{1}{2}((8k + c)n - 1)$$

za neko naravno število k. Naj bo $b = 8k + c$. Potem je $b > 0$ in $2p = bn - 1$ ter velja

$$
\left.
\begin{aligned}
&b \equiv 3 \pmod 8 \ in \ p \equiv 1 \pmod 4 \ za \ n \equiv 1 \pmod 8,\\
&b \equiv 1 \pmod 8 \ in \ p \equiv 1 \pmod 4 \ za \ n \equiv 3 \pmod 8,\\
&b \equiv 3 \pmod 8 \ in \ p \equiv 3 \pmod 4 \ za \ n \equiv 5 \pmod 8.
\end{aligned}
\right\} \qquad (4.2)
$$

Izračun za Jacobijev simbol

$$\begin{aligned}
\left(\frac{-b}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{b}{p}\right) \text{ po točki (2.9) Izreka 2.25} \\
&= \left(-1\right)^{\frac{p-1}{2}}\left(\frac{b}{p}\right) \text{ po Izreku 2.27} \\
&= \left(-1\right)^{\frac{p-1}{2}}\left(-1\right)^{\frac{p-1}{2}\frac{b-1}{2}}\left(\frac{p}{b}\right) \text{ po Izreku 2.26} \\
&= \left(\frac{p}{b}\right) \text{ po enačbi (4.2)} \\
&= \left(\frac{p}{b}\right)\left(\frac{-2}{b}\right) \text{ po Izreku 2.29} \\
&= \left(\frac{-2p}{b}\right) \text{ po točki (2.9) Izreka 2.25} \\
&= \left(\frac{-bn+1}{b}\right), \text{ ker je } 2p = bn-1 \\
&= \left(\frac{1}{b}\right) \text{ po Lemi 2.24} \\
&= 1.
\end{aligned}$$

Torej je tudi v tem primeru $-b$ kvadratni ostanek praštevila p, kar pomeni, da ima kvadratna kongruenca $x^2 \equiv -b \pmod{p}$ rešitev. Sedaj bomo pokazali, da ima tudi kongruenca $x^2 \equiv -b \pmod{2p}$ rešitev. Naj bo x_1 rešitev kongruence $x^2 \equiv -b \pmod{p}$. Hitro opazimo, da je v tem primeru turi $p - x_1$ rešitev kongruence $x^2 \equiv -b \pmod{p}$, ter da je natanko eden izmed x_1 in $p - x_1$ liho število. Torej ima kongruenca $x^2 \equiv -b \pmod{p}$ vedno rešitev x_2, ki je liho število.

Ker je x_2 rešitev kongruence $x^2 \equiv -b \pmod{p}$, obstaja tako celo število k, da je $x_2^2 + b = kp$. Ker so x_2, b in p vsa liha števila, mora biti k sodo število, torej je $k = 2k_1$ za neko celo število k_1. Torej je $x_2^2 + k = 2k_1p$, kar pomeni, da $2p$ deli $x_2^2 + b$, oziroma, da je kongruenca $x^2 \equiv -b \pmod{2p}$ rešljiva.

Koeficient a_{12} naj bo ena od rešitev kvadratne kongruence $x^2 \equiv -b \pmod{2p}$. Torej je a_{12} celo število. Koeficient $a_{22} = bn - 1$ je pravtako celo število, saj sta b in n celi števili. Za koeficient a_{11} pa velja

$$a_{11} = \frac{b + a_{12}^2}{a_{22}} = \frac{b + a_{12}^2}{bn - 1} = \frac{b + a_{12}^2}{2p}.$$

Ker je a_{12} rešitev kongruence $x^2 \equiv -b \pmod{2p}$, je število $b + a_{12}^2$ deljivo z $2p$, in je torej tudi koeficient a_{11} celo število. □

5 PREDSTAVITEV NARAVNIH ŠTEVIL KOT VSOTE ŠTIRIH KVADRATOV

Skoraj vsa števila lahko zapišemo kot vsoto treh kvadratov, razen tistih, ki so oblike $4^x(8y+7)$ za neki nenegativni celi števili x in y. Naravno vprašanje je torej ali je zanje dovolj vsota štirih kvadratov? Prvi matematik, ki se je ukvarjal s tem je bil Bachet, ki je trdil, da lahko vsako število predstavimo kot vsoto štirih kvadratov, kjer je vključen kvadrat tudi 0^2. Leta 1621 je objavil prvih 325 naravnih števil ter njihove zapise kot vsote štirih kvadratov. Petnajst let za njim je Fermat trdil, da je dokazal njegovo tezo, vendar dokaz ni bil objavljen. Šele leta 1772 je Lagrange objavil dokaz, da lahko res vsako število zapišemo kot vsoto štirih kvadratov.
V dokazu bomo potrebovali Eulerjevo lemo, ki pravi, da če imamo dve števili, ki ju lahko zapišemo kot vsoto štirih kvadratov, potem lahko tudi njun produkt zapišemo kot vsoto štirih kvadratov, ter dejstvo, da lahko vsako praštevilo zapišemo kot vsoto štirih kvadratov. Izreki, leme ter posledice so povzete po [1].

Lema 5.1. *(EULERJEVA LEMA) Če lahko naravni števili m in n zapišemo kot vsoto štirih kvadratov, potem lahko tudi njun produkt mn zapišemo kot vsoto štirih kvadratov.*

Dokaz. Če je

$$m = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

in

$$n = b_1^2 + b_2^2 + b_3^2 + b_4^2$$

za cela števila a_i in b_j, potem velja

$$\begin{aligned} mn &= (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\ &= (a_1b_1)^2 + (a_1b_2)^2 + (a_1b_3)^2 + (a_1b_4)^2 + (a_2b_1)^2 + (a_2b_2)^2 + (a_2b_3)^2 + (a_2b_4)^2 \\ &+ (a_3b_1)^2 + (a_3b_2)^2 + (a_3b_3)^2 + (a_3b_4)^2 + (a_4b_1)^2 + (a_4b_2)^2 + (a_4b_3)^2 + (a_4b_4)^2 \\ &= (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 \\ &+ (a_1b_3 - a_2b_4 - a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 - a_4b_1)^2. \end{aligned}$$

□

Primer 5.2. Oglejmo si števili 15 ter 46, kateri lahko obe zapišemo kot vsoto štirih kvadratov

$$15 = 3^2 + 2^2 + 1^2 + 1^2 \quad in \quad 46 = 5^2 + 4^2 + 2^2 + 1^2.$$

Iz tega sledi, da lahko tudi število 690 zapišemo kot vsoto štirih kvadratov, saj je $690 = 15 \cdot 46$.

$$\begin{aligned} 690 &= (3\cdot 5 + 2\cdot 4 + 1\cdot 2 + 1\cdot 1)^2 + (3\cdot 4 - 2\cdot 5 + 1\cdot 1 - 1\cdot 2)^2 \\ &+ (3\cdot 2 - 2\cdot 1 - 1\cdot 5 + 1\cdot 4)^2 + (3\cdot 1 + 2\cdot 2 - 1\cdot 4 - 1\cdot 5)^2 \\ &= 26^2 + 1^2 + 3^2 + (-2)^2. \end{aligned}$$

■

Za dokaz izreka, da lahko vsako praštevilo zapišemo kot vsoto štirih kvadratov, potrebujemo dodatno lemo, ki pravi, da če imamo liho praštevilo p, potem ima kongruenca $x^2 + y^2 + 1 \equiv 0 \ (mod\ p)$ rešitev x_0, y_0, za katero velja $0 \leq x_0 \leq \frac{p-1}{2}$ in $0 \leq y_0 \leq \frac{p-1}{2}$. Iz leme izpeljemo še posledico, ki pravi, da za dano liho praštevilo p obstaja celo število $k < p$, tako da lahko tudi kp zapišemo kot vsoto štirih kvadratov.

Lema 5.3. *Če je p liho praštevilo, potem ima kongruenca*

$$x^2 + y^2 + 1 \equiv 0 \ (mod\ p)$$

rešitev x_0, y_0, za katero velja $0 \leq x_0 \leq \frac{p-1}{2}$ in $0 \leq y_0 \leq \frac{p-1}{2}$.

Dokaz. Oglejmo si množici

$$S_1 = \left\{1 + 0^2, 1 + 1^2, 1 + 2^2, \ldots, 1 + \left(\frac{p-1}{2}\right)^2\right\}$$

in

$$S_2 = \left\{-0^2, -1^2, -2^2, \ldots, -\left(\frac{p-1}{2}\right)^2\right\}.$$

Očitno velja, da nobena dva elementa množice S_1 nista kongruentna po modulu p. Saj, če je $1 + x_1^2 \equiv 1 + x_2^2 \ (mod\ p)$, za x_1 in x_2 med 0 in $\frac{p-1}{2}$, potem velja $x_1 \equiv x_2 \ (mod\ p)$ ali $x_1 \equiv -x_2 \ (mod\ p)$. Zadnja ekvivalenca $x_1 \equiv -x_2 \ (mod\ p)$ ni mogoča, saj je $0 < x_1 + x_2 < p$, torej velja $x_1 \equiv x_2 \ (mod\ p)$. Iz tega sledi, da je $x_1 = x_2$. Popolnoma enak sklep naredimo za množico S_2, torej nobena dva elementa iz množice S_2 nista kongruentna po modulu p.
Množici S_1 in S_2 imata skupaj $2\left(1 + \frac{1}{2}(p-1)\right) = p + 1$ elementov. Po principu golobnjaka (Izrek 3.7), zato obstaja neko število iz množice S_1, ki je kongruentno po modulu p nekemu številu iz množice S_2. Torej obstaja x_0, y_0 tako da

$$1 + x_0^2 \equiv -y_0^2 \ (mod\ p),$$

kjer je $0 \leq x_0 \leq \frac{p-1}{2}$ in $0 \leq y_0 \leq \frac{p-1}{2}$. □

Posledica 5.4. *Za dano liho praštevilo p obstaja celo število $k < p$, tako da lahko kp zapišemo kot vsoto štirih kvadratov.*

Dokaz. Po Lemi 5.3 obstajata števili x_0 in y_0, ki zadoščata pogojem

$$0 \leq x_0 < \frac{p}{2},\ 0 \leq y_0 < \frac{p}{2}, \tag{5.1}$$

tako da velja

$$x_0^2 + y_0^2 + 1^2 + 0^2 = kp$$

za nek primeren k. Iz pogojev (5.1) sledi

$$kp = x_0^2 + y_0^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2.$$

Torej je res $k < p$. □

Primer 5.5. Oglejmo si primer, ko je $p = 13$. Potem sta množici S_1 ter S_2 sledeči

$$S_1 = \{1, 2, 5, 10, 17, 26, 37\}$$

$$S_2 = \{0, -1, -4, -9, -16, -25, -36\}.$$

Po modulu 13 so elementi množice S_1 enaki 1, 2, 5, 10, 4, 0, 11 in elementi množice S_2 enaki 0, 12, 9, 4, 10, 1, 3. Po Lemi 5.3 obstaja element množice S_1, ki je oblike $1 + x^2$, ki je kongruenten po modulu 13 elementu, ki je oblike $-y^2$, iz množice S_2. Torej velja

$$17 = 1 + 4^2 \equiv 4 \equiv -3^2 \ \ (mod\ 13)$$

oziroma

$$1 + 4^2 + 3^2 \equiv 0 \ \ (mod\ 13).$$

Od koder sledi

$$2 \cdot 13 = 1^2 + 4^2 + 3^2 + 0^2.$$

Pravtako velja

$$17 = 1 + 4^2 \equiv 4 \equiv -5^2 - 6^2 \ \ (mod\ 13)$$

oziroma

$$1 + 4^2 + 5^2 + 6^2 \equiv 0 \ \ (mod\ 13).$$

Od koder sledi

$$6 \cdot 13 = 1^2 + 4^2 + 5^2 + 6^2.$$

Obstaja še več možnosti, torej lahko poiščemo še več večkratnikov števila 13, katere lahko zapišemo kot vsoto štirih kvadratov. ■

Izrek 5.6. *Vsako praštevilo p lahko zapišemo kot vsoto štirih kvadratov.*

Dokaz. Očitno izrek velja za praštevilo $p = 2$, saj je $2 = 1^2 + 1^2 + 0^2 + 0^2$. Torej lahko dokaz nadaljujemo za liha praštevila. Naj bo k najmanjše pozitivno celo število, tako da lahko kp zapišemo kot vsoto štirih kvadratov

$$kp = x^2 + y^2 + z^2 + w^2. \tag{5.2}$$

Zaradi Posledice 5.2 velja, da je $k < p$. Torej je naš cilj dokazati, da je $k = 1$.
Najprej bomo s pomočjo protislovja dokazali, da je k liho število. Torej recimo, da je k sodo število. Potem so x, y, z, w ali vsa soda števila, ali vsa liha števila ali dve sodi in dve lihi števili. V vsakem primeru lahko predpostavimo

$$x \equiv y \pmod 2 \quad in \quad z \equiv w \pmod 2.$$

Od tod sledi, da so

$$\frac{1}{2}(x-y), \quad \frac{1}{2}(x+y), \quad \frac{1}{2}(z-w), \quad \frac{1}{2}(z+w)$$

vsa cela števila in velja

$$\frac{1}{2}(kp) = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2,$$

kar je predstavitev števila $(\frac{k}{2})p$ kot vsota štirih kvadratov. Kar je v protislovju z našo predpostavko, da je k najmnajše število, da lahko kp zapišemo kot vsoto štirih kvadratov. Torej je k liho število.
Predpostavimo, da je k liho število večje ali enako 3. Zato lahko izberemo števila a, b, c, d, tako da

$$a \equiv x \pmod k,\ b \equiv y \pmod k,$$

$$c \equiv z \pmod k,\ d \equiv w \pmod k$$

in velja

$$|a| < \frac{k}{2}, \quad |b| < \frac{k}{2}, \quad |c| < \frac{k}{2}, \quad |d| < \frac{k}{2}. \tag{5.3}$$

Iz tega sledi

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \pmod k,$$

torej je

$$a^2 + b^2 + c^2 + d^2 = nk \tag{5.4}$$

za neko nenegativno celo število n. Iz (5.3) in (5.4) sledi

$$0 \leq nk = a^2 + b^2 + c^2 + d^2 < 4\left(\frac{k}{2}\right)^2 = k^2.$$

Če bi bil $n = 0$, potem bi sledilo, da so $a = b = c = d = 0$, kar pa posledično pomeni, da k deli števila x, y, z, w. Potem velja $k^2|kp$ oziroma $k|p$, kar je nemogoče, saj $1 < k < p$. Iz neenakosti $nk < k^2$ sledi, da je $n < k$. Iz (5.2) in (5.4) sledi

$$\begin{aligned} k^2np &= (kp)(nk) = (x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) = \\ &= r^2 + s^2 + t^2 + u^2, \end{aligned}$$

kjer je

$$r = xa + yb + zc + wd,$$

$$s = xb - ya + zd - wc,$$

$$t = xc - yd - za + wb,$$

$$u = xd + yc - zb - wa.$$

Pomembna opazka je, da so vsi r, s, t, u deljivi s k. Oglejmo si ta števila

$$r = xa + yb + zc + wd \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{k},$$

$$s = xb - ya + zd - wc \equiv ab - ba + cd - dc = 0 \pmod{k},$$

$$t = xc - yd - za + wb \equiv ac - bd - ca + db = 0 \pmod{k},$$

$$u = xd + yc - zb - wa \equiv ad + bc - cb - da = 0 \pmod{k}.$$

Kar nas pripelje do

$$np = \left(\frac{r}{k}\right)^2 + \left(\frac{s}{k}\right)^2 + \left(\frac{t}{k}\right)^2 + \left(\frac{u}{k}\right)^2,$$

kjer so $\frac{r}{k}, \frac{s}{k}, \frac{t}{k}, \frac{u}{k}$ vsa cela števila. Ker je $0 < n < k$, nas to pripelje do protislovja, da je k najmanjše število, da lahko kp zapišemo kot vsoto štirih kvadratov. Torej je $k = 1$ in smo s tem zaključili dokaz. □

Najpomembnejši izrek je torej Lagrangev izrek, ki sledi v nadaljevanju, in pravi, da lahko vsako naravno število zapišemo kot vsoto štirih kvadratov, pri čemer so nekateri lahko enaki 0.

Izrek 5.7. *(LAGRANGEV IZREK) Vsako naravno število n lahko zapišemo kot vsoto štirih kvadratov, pri čemer so nekateri lahko enaki 0.*

Dokaz. Očitno velja za $1 = 1^2 + 0^2 + 0^2 + 0^2$, da ga lahko zapišemo kot vsoto štirih kvadratov. Predpostavimo, da je $n > 1$ in $n = p_1p_2 \cdots p_r$ prafaktorski razcep za število n. Po Izreku 5.6 lahko vsak p_i zapišemo kot vsoto štirih kvadratov. Zaradi Leme 5.1 vemo, da lahko produkt dveh števil, kateri lahko vsako posebej zapišemo kot vsoto štirih kvadratov, pravtako zapišemo kot vsoto štirih kvadratov. Torej po indukciji lahko vsako število, ki je končen produkt praštevil, zapišemo kot vsoto štirih kvadratov. □

Dokaz, da lahko vsako naravno število zapišemo kot vsoto štirih kvadratov smo izpeljali neodvisno od 4. poglavja. Seveda lahko ta izrek dokažemo tudi na drug način, kjer uporabimo ugotovitve iz 4. poglavja.

Dokaz. Naj bo n naravno število, ki ni oblike $4^x(8y+7)$, kjer sta x in y nenegativni celi števili. Potem po Izreku 4.15 velja, da ga lahko zapišemo kot vsoto treh kvadratov. Torej obstajajo cela števila a, b, c, tako da velja $n = a^2 + b^2 + c^2$. Torej velja, da lahko n zapišemo kot vsoto štirih kvadratov na sledeč način:

$$n = a^2 + b^2 + c^2 + 0^2.$$

Oglejmo si še primer, ko je $n = 4^x(8y+7)$ za neki nenegativni celi števili x in y.

$$n = 4^x(8y+7) = 4^x(8y+6) + 4^x = 4^x(8y+6) + (2^2)^x = 4^x(8y+6) + (2^x)^2. \quad (5.5)$$

Število $4^x(8y+6)$ lahko prav tako po Izreku 4.15 zapišemo kot vsoto treh kvadratov, saj ni oblike $4^x(8y+7)$. Torej obstajajo cela števila a, b, c, tako da velja

$$4^x(8y+6) = a^2 + b^2 + c^2. \quad (5.6)$$

Nadaljujemo z enačbo (5.5), pri čemer upoštevamo enačbo (5.6)

$$n = 4^x(8y+6) + (2^x)^2 = a^2 + b^2 + c^2 + (2^x)^2.$$

S tem smo dokazali, da lahko n zapišemo kot vsoto štirih kvadratov tudi v primeru, ko je oblike $4^x(8y+7)$. □

6 ŠTEVILO REPREZENTACIJ NARAVNEGA ŠTEVILA KOT VSOTE KVADRATOV

Ne samo, da lahko vsako naravno število zapišemo kot vsoto štirih kvadratov, vemo tudi na koliko načinov lahko to naredimo. Leta 1829 je Jacobi dokazal, da je število načinov zapisa naravnega števila n kot vsote štirih kvadratov osemkratnik vsote deliteljev števila n, ki niso deljivi s 4. Pri štetju načinov dovoljujemo, da so členi v vsoti ne samo kvadrati naravnih števil, ampak tudi kvadrati celih števil. S formulo to zapišemo

$$r_4(n) := \#\left\{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 | \sum_{i=1}^{4} x_i^2 = n\right\} = 8\left(\sum_{d|n} d - \sum_{4d|n} 4d\right). \tag{6.1}$$

Celotno poglavje je povzeto po [5].

Primer 6.1. Oglejmo si primer, ko je $n = 1$. Delitelj števila 1 je samo 1, torej po formuli (6.1)

$$r_4(1) = 8(1 - 0) = 8.$$

Torej lahko število 1 zapišemo na osem različnih načinov kot vsoto štirih kvadratov:

$$\begin{aligned} 1 &= 1^2 + 0^2 + 0^2 + 0^2 \\ &= 0^2 + 1^2 + 0^2 + 0^2 \\ &= 0^2 + 0^2 + 1^2 + 0^2 \\ &= 0^2 + 0^2 + 0^2 + 1^2 \\ &= (-1)^2 + 0^2 + 0^2 + 0^2 \\ &= 0^2 + (-1)^2 + 0^2 + 0^2 \\ &= 0^2 + 0^2 + (-1)^2 + 0^2 \\ &= 0^2 + 0^2 + 0^2 + (-1)^2. \end{aligned}$$

■

Oglejmo si Jacobijev dokaz za zgornjo formulo. Najprej si oglejmo

$$\left(\sum_{n=-\infty}^{\infty} x^{n^2}\right)^4 = \left(\sum_{n=-\infty}^{\infty} x^{n^2}\right) \cdot \left(\sum_{n=-\infty}^{\infty} x^{n^2}\right) \cdot \left(\sum_{n=-\infty}^{\infty} x^{n^2}\right) \cdot \left(\sum_{n=-\infty}^{\infty} x^{n^2}\right) =$$

$$= 1 + r_4(1)x + r_4(2)x^2 + \cdots = 1 + \sum_{l=1}^{\infty} r_4(l)x^l. \tag{6.2}$$

Oglejmo si še dve vsoti. Najprej iz dobro znane enačbe za vsoto neskončne geometrijekse vrste dobimo:

$$\sum_{n=1}^{\infty}(x^n)^k = \frac{x^n}{1-x^n}.$$

Sedaj lahko izpeljemo naslednje

$$\sum_{n=1}^{\infty}\frac{nx^n}{1-x^n} = \sum_{n=1}^{\infty} n\frac{x^n}{1-x^n} = \sum_{n=1}^{\infty} n\sum_{k=1}^{\infty}(x^n)^k = \sum_{n=1}^{\infty}\sum_{k=1}^{\infty} nx^{nk} = \sum_{l=1}^{\infty}\sum_{d|l} dx^l. \tag{6.3}$$

Podobno velja tudi za naslednjo vsoto

$$\sum_{n=1}^{\infty}\frac{4nx^{4n}}{1-x^{4n}} = \sum_{n=1}^{\infty} 4n\frac{x^{4n}}{1-x^{4n}} = \sum_{n=1}^{\infty} 4n\sum_{k=1}^{\infty}(x^{4n})^k =$$

$$= \sum_{n=1}^{\infty}\sum_{k=1}^{\infty} 4nx^{4nk} = \sum_{l=1}^{\infty}\sum_{4d|l} 4dx^l. \tag{6.4}$$

Če združimo enačbe (6.2), (6.3) in (6.4) bi bilo za dokaz naše formule dovolj dokazati

$$\left(\sum_{n=-\infty}^{\infty} x^{n^2}\right)^4 = 1 + 8\left(\sum_{n=1}^{\infty}\frac{nx^n}{1-x^n} - \sum_{n=1}^{\infty}\frac{4nx^{4n}}{1-x^{4n}}\right). \tag{6.5}$$

Enačbo (6.5) dokažemo s pomočjo naslednjih sedmih enakosti.

1. $$\sum_{n=-\infty}^{\infty}(-1)^n x^{n^2} = \prod_{n=1}^{\infty}\frac{1-x^n}{1+x^n}.$$

2. $$\prod_{n=1}^{\infty}(1-x^{2n})(1+zx^{2n-1})(1+z^{-1}x^{2n-1}) = \sum_{n=-\infty}^{\infty} z^n x^{n^2}.$$

3. $$(z-z^{-1})\prod_{n=1}^{\infty}(1-x^n)(1-z^2x^n)(1-z^{-2}x^n) = \sum_{n=-\infty}^{\infty}(-1)^n z^{2n+1}x^{\frac{n(n+1)}{2}}.$$

4. $$\prod_{n=1}^{\infty}(1-x^n)^3 = \frac{1}{2}\sum_{n=-\infty}^{\infty}(2n+1)(-1)^n x^{\frac{n(n+1)}{2}}.$$

5. $$\prod_{n=1}^{\infty}(1-x^n)^6 = \frac{1}{2}\sum_{r,s=-\infty}^{\infty}((2r+1)^2-(2s)^2)x^{r^2+r+s^2}.$$

6.
$$\prod_{n=1}^{\infty}(1-x^n)^6 = \prod_{n=1}^{\infty} Q_n \cdot \left(1 - 8\sum_{n=1}^{\infty}\left(\frac{(2n-1)x^{2n-1}}{1+x^{2n-1}} - \frac{2nx^{2n}}{1+x^{2n}}\right)\right),$$
$$\textit{kjer je } Q_n = (1-x^{2n})^2(1+x^{2n})^2(1+x^{2n-1})^2.$$

7.
$$\prod_{n=1}^{\infty}(1+x^n)^4(1-x^n)^2 = \prod_{n=1}^{\infty} Q_n.$$

Privzemimo najprej, da zgornje enakosti res veljajo. Enačbo 1. damo najprej na četrto potenco. Desna stran dobljene enačbe je enaka količniku enačbe 6. in enačbe 7.

$$\left(\sum_{n=-\infty}^{\infty}(-1)^n x^{n^2}\right)^4 = \prod_{n=1}^{\infty}\left(\frac{1-x^n}{1+x^n}\right)^4 = \frac{\textit{leva stran enačbe 6.}}{\textit{leva stran enačbe 7.}} =$$

$$= \frac{\prod_{n=1}^{\infty}(1-x^n)^6}{\prod_{n=1}^{\infty}(1+x^n)^4(1-x^n)^2} = 1 - 8\sum_{n=1}^{\infty}\left(\frac{(2n-1)x^{2n-1}}{1+x^{2n-1}} - \frac{2nx^{2n}}{1+x^{2n}}\right).$$

V dobljeno enakost vstavimo $x = -x$ in dobimo

$$\left(\sum_{n=-\infty}^{\infty}(-1)^n(-x)^{n^2}\right)^4 = 1 - 8\sum_{n=1}^{\infty}\left(\frac{(2n-1)(-x)^{2n-1}}{1+(-x)^{2n-1}} - \frac{2n(-x)^{2n}}{1+(-x)^{2n}}\right),$$

$$\left(\sum_{n=-\infty}^{\infty}x^{n^2}\right)^4 = 1 - 8\sum_{n=1}^{\infty}\left(-\frac{(2n-1)x^{2n-1}}{1-x^{2n-1}} - \frac{2nx^{2n}}{1+x^{2n}}\right),$$

$$\left(\sum_{n=-\infty}^{\infty}x^{n^2}\right)^4 = 1 + 8\sum_{n=1}^{\infty}\left(\frac{(2n-1)x^{2n-1}}{1-x^{2n-1}} + \frac{2nx^{2n}}{1+x^{2n}}\right). \tag{6.6}$$

Dobljena enačba je že zelo podobna enačbi 6.5, ki jo dokazujemo. Poračunajmo zadnjo vsoto.

$$\sum_{n=1}^{\infty}\left(\frac{(2n-1)x^{2n-1}}{1-x^{2n-1}} + \frac{2nx^{2n}}{1+x^{2n}}\right) =$$

$$= \sum_{n=1}^{\infty}\left(\frac{(2n-1)x^{2n-1}}{1-x^{2n-1}} + \frac{2nx^{2n}}{1-x^{2n}}\right) - \sum_{n=1}^{\infty}\left(\frac{2nx^{2n}}{1-x^{2n}} - \frac{2nx^{2n}}{1+x^{2n}}\right). \tag{6.7}$$

Prva vsota v dobljeni razliki je enaka

$$\sum_{n=1}^{\infty}\left(\frac{(2n-1)x^{2n-1}}{1-x^{2n-1}} + \frac{2nx^{2n}}{1-x^{2n}}\right) =$$

$$= \frac{x}{1-x} + \frac{2x^2}{1-x^2} + \frac{3x^3}{1-x^3} + \frac{4x^4}{1-x^4} + \cdots = \sum_{n=1}^{\infty}\frac{nx^x}{1-x^n}. \tag{6.8}$$

Druga vsota v razliki je enaka

$$\sum_{n=1}^{\infty}\left(\frac{2nx^{2n}}{1-x^{2n}} - \frac{2nx^{2n}}{1+x^{2n}}\right) = \sum_{n=1}^{\infty}\left(\frac{(2nx^{2n})(1+x^{2n}) - (2nx^{2n})(1-x^{2n}))}{(1-x^{2n})(1+x^{2n})}\right) =$$

$$= \sum_{n=1}^{\infty} \left(\frac{2nx^{2n} + 2nx^{4n} - 2nx^{2n} + 2nx^{4n}}{1 - x^{4n}} \right) = \sum_{n=1}^{\infty} \left(\frac{4nx^{4n}}{1 - x^{4n}} \right). \tag{6.9}$$

Dobljene rezultate enačbo (6.7), enačbo (6.8) in enačbo (6.9) vstavimo v enačbo (6.6) ter dobimo

$$\left(\sum_{n=-\infty}^{\infty} x^{n^2} \right)^4 = 1 + 8 \left(\sum_{n=1}^{\infty} \frac{nx^n}{1 - x^n} - \sum_{n=1}^{\infty} \frac{4nx^{4n}}{1 - x^{4n}} \right),$$

kar je natanko enačba (6.5), katero smo želeli dokazati.

Sedaj si oglejmo dokaze pomožnih sedmih enačb, katere smo uporabili v dokazu enačbe (6.5). Enačbae 2. v tem magistrskem delu ne bomo dokazali. Zainteresirani bralec lahko dokaz najde recimo v [5]. Bomo pa iz enačbe 2. izpeljali vseh preostalih šest enačb.

2. $\Rightarrow$ 1.: Če v enačbo 2. vstavimo $z = -1$, dobimo

$$\prod_{n=1}^{\infty} (1 - x^{2n})(1 + (-1)x^{2n-1})(1 + (-1)^{-1}x^{2n-1}) = \sum_{n=-\infty}^{\infty} (-1)^n x^{n^2},$$

oziroma

$$\prod_{n=1}^{\infty} (1 - x^{2n})(1 - x^{2n-1})^2 = \sum_{n=-\infty}^{\infty} (-1)^n x^{n^2}. \tag{6.10}$$

Vemo, da velja

$$1 - x^{2n} = (1 - x^n)(1 + x^n),$$

torej je

$$1 - x^n = \frac{1 - x^{2n}}{1 + x^n}. \tag{6.11}$$

Opazimo tudi, da velja

$$\prod_{n=1}^{\infty} (1 - x^{2n})(1 - x^{2n-1}) = (1 - x^2)(1 - x^1)(1 - x^4)(1 - x^3) \cdots = \prod_{n=1}^{\infty} (1 - x^n). \tag{6.12}$$

Če (6.11) in (6.12) vstavimo v levo stran enačbe (6.10) ter poenostavimo, dobimo

$$\begin{aligned}
\prod_{n=1}^{\infty} (1 - x^{2n})(1 - x^{2n-1})^2 &= \prod_{n=1}^{\infty} (1 - x^{2n})(1 - x^{2n-1})(1 - x^{2n-1}) \\
&= \prod_{n=1}^{\infty} (1 - x^n)(1 - x^{2n-1}) \\
&= \prod_{n=1}^{\infty} \frac{(1 - x^{2n})}{(1 + x^n)} (1 - x^{2n-1}) \\
&= \prod_{n=1}^{\infty} \frac{(1 - x^n)}{(1 + x^n)}.
\end{aligned}$$

Torej iz enačbe (6.10) sledi, da je $\prod_{n=1}^{\infty} \frac{(1-x^n)}{(1+x^n)} = \sum_{n=-\infty}^{\infty} (-1)^n x^{n^2}$.

2. $\Rightarrow$ 3.: Najprej v enačbo 2. vstavimo $z = -xz^2$ ter dobimo

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+(-xz^2)x^{2n-1})(1+(-xz^2)^{-1}x^{2n-1}) = \sum_{n=-\infty}^{\infty}(-xz^2)^n x^{n^2},$$

oziroma

$$\prod_{n=1}^{\infty}(1-x^{2n})(1-z^2x^{2n})(1-z^{-2}x^{2n-2}) = \sum_{n=-\infty}^{\infty}(-1)^n z^{2n} x^{n^2+n}.$$

Nato v dobljeno enačbo vstavimo $x = x^{\frac{1}{2}}$ ter dobimo

$$\prod_{n=1}^{\infty}(1-x^{n})(1-z^2x^{n})(1-z^{-2}x^{n-1}) = \sum_{n=-\infty}^{\infty}(-1)^n z^{2n} x^{\frac{n^2+n}{2}}.$$

Na koncu dobljeno enačbo še pomnožimo z z. Od tod sledi

$$z\prod_{n=1}^{\infty}(1-x^{n})(1-z^2x^{n})(1-z^{-2}x^{n-1}) = z\sum_{n=-\infty}^{\infty}(-1)^n z^{2n} x^{\frac{n^2+n}{2}}.$$

Levo stran enačbe preoblikujemo

$$z\prod_{n=1}^{\infty}(1-x^{n})(1-z^2x^{n})(1-z^{-2}x^{n-1}) =$$

$$= z\left(\prod_{n=1}^{\infty}(1-x^n)\right)\left(\prod_{n=1}^{\infty}(1-z^2x^n)\right)\left(\prod_{n=1}^{\infty}(1-z^{-2}x^{n-1})\right) =$$

$$= z\left(\prod_{n=1}^{\infty}(1-x^n)\right)\left(\prod_{n=1}^{\infty}(1-z^2x^n)\right)(1-z^{-2})\left(\prod_{n=2}^{\infty}(1-z^{-2}x^{n-1})\right) =$$

$$= z(1-z^{-2})\left(\prod_{n=1}^{\infty}(1-x^n)\right)\left(\prod_{n=1}^{\infty}(1-z^2x^n)\right)\left(\prod_{n=2}^{\infty}(1-z^{-2}x^{n-1})\right) =$$

$$= z(1-z^{-2})\left(\prod_{n=1}^{\infty}(1-x^n)\right)\left(\prod_{n=1}^{\infty}(1-z^2x^n)\right)\left(\prod_{n=1}^{\infty}(1-z^{-2}x^{n})\right) =$$

$$= (z-z^{-1})\prod_{n=1}^{\infty}(1-x^n)(1-z^2x^n)(1-z^{-2}x^n).$$

Torej res velja

$$(z-z^{-1})\prod_{n=1}^{\infty}(1-x^{n})(1-z^2x^{n})(1-z^{-2}x^{n}) = \sum_{n=-\infty}^{\infty}(-1)^n z^{2n+1} x^{\frac{n(n+1)}{2}}.$$

3. $\Rightarrow$ 4.: Enačbo 3. odvajamo po z in dobimo

$$\frac{d}{dz}(z-z^{-1})\cdot\prod_{n=1}^{\infty}(1-x^n)(1-z^2x^n)(1-z^{-2}x^n)$$

$$+(z-z^{-1})\cdot\frac{d}{dz}\left(\prod_{n=1}^{\infty}(1-x^n)(1-z^2x^n)(1-z^{-2}x^n)\right)=$$

$$=\frac{d}{dz}\left(\sum_{n=-\infty}^{\infty}(-1)^n z^{2n+1}x^{\frac{n(n+1)}{2}}\right).$$

Iz pravil za odvajanje sledi, da velja

$$(1+z^{-2})\cdot\prod_{n=1}^{\infty}(1-x^n)(1-z^2x^n)(1-z^{-2}x^n)$$

$$+(z-z^{-1})\cdot\frac{d}{dz}\left(\prod_{n=1}^{\infty}(1-x^n)(1-z^2x^n)(1-z^{-2}x^n)\right)=$$

$$=\sum_{n=-\infty}^{\infty}(-1)^n(2n+1)z^{2n}x^{\frac{n(n+1)}{2}}.$$

V dobljeno enačbo vstavimo $z=1$, od koder sledi, da je

$$2\prod_{n=1}^{\infty}(1-x^n)(1-x^n)(1-x^n)=\sum_{n=-\infty}^{\infty}(-1)^n(2n+1)x^{\frac{n(n+1)}{2}}.$$

Enačbo še pomnožimo z $\frac{1}{2}$

$$\prod_{n=1}^{\infty}(1-x^n)^3=\frac{1}{2}\sum_{n=-\infty}^{\infty}(-1)^n(2n+1)x^{\frac{n(n+1)}{2}}$$

in res dobimo enačbo 4.

4. $\Rightarrow$ 5.: Najprej enačbo 4. kvadriramo. Tako dobimo

$$\prod_{n=1}^{\infty}(1-x^n)^6=\frac{1}{4}\sum_{m,n=-\infty}^{\infty}(2m+1)(2n+1)(-1)^{m+n}x^{\frac{m^2+m+n^2+n}{2}}. \tag{6.13}$$

Dobljeno vsoto razdelimo na dve vsoti. V prvi zajamemo vse člene, za katere velja, da je $m+n$ sodo število, ter v drugi zajamemo vse člene, za katere velja, da je $m+n$ liho število. V prvo vsoto vpeljemo novi oznaki $r=\frac{m+n}{2}$ in $s=\frac{m-n}{2}$, ter v drugo vpeljemo oznaki $r=\frac{m-n-1}{2}$ in $s=\frac{m+n+1}{2}$.

$$\sum_{m,n=-\infty}^{\infty}(2m+1)(2n+1)(-1)^{m+n}x^{\frac{m^2+m+n^2+n}{2}}=$$

$$=\sum_{m+n\ sod}(2m+1)(2n+1)(-1)^{m+n}x^{\frac{m^2+m+n^2+n}{2}}$$

$$+ \sum_{m+n\ lih} (2m+1)(2n+1)(-1)^{m+n} x^{\frac{m^2+m+n^2+n}{2}} =$$

$$= \sum_{r,s=-\infty}^{\infty} (2(r+s)+1)(2(r-s)+1) x^{\frac{(r+s)^2+(r+s)+(r-s)^2+(r-s)}{2}}$$

$$+ \sum_{r,s=-\infty}^{\infty} (2(r+s)+1)(2(s-r-1)+1)(-1) x^{\frac{(r+s)^2+(r+s)+(s-r-1)^2+(s-r-1)}{2}} =$$

$$= \sum_{r,s=-\infty}^{\infty} ((2r+1)^2 - (2s)^2) x^{2(r^2+r+s^2)} + \sum_{r,s=-\infty}^{\infty} ((2r+1)^2 - (2s)^2) x^{2(r^2+r+s^2)} =$$

$$= 2 \cdot \sum_{r,s=-\infty}^{\infty} ((2r+1)^2 - (2s)^2) x^{2(r^2+r+s^2)}.$$

Dobljeno enakost vstavimo v (6.13)

$$\prod_{n=1}^{\infty} (1-x^n)^6 = \frac{1}{4} \cdot 2 \cdot \sum_{r,s=-\infty}^{\infty} ((2r+1)^2 - (2s)^2) x^{2(r^2+r+s^2)} =$$

$$= \frac{1}{2} \sum_{r,s=-\infty}^{\infty} ((2r+1)^2 - (2s)^2) x^{2(r^2+r+s^2)},$$

kar je natanko enačba 5.

2. in 5. $\Rightarrow$ 6.: Začnemo z enačbo 5. ter njeno desno stran zapišemo kot razliko dveh vsot

$$\prod_{n=1}^{\infty} (1-x^n)^6 = \frac{1}{2} \sum_{r,s=-\infty}^{\infty} ((2r+1)^2 - (2s)^2) x^{r^2+r+s^2} =$$

$$= \frac{1}{2} \left(\sum_{r,s=-\infty}^{\infty} (2r+1)^2 x^{r^2+r+s^2} - \sum_{r,s=-\infty}^{\infty} (2s)^2 x^{r^2+r+s^2} \right).$$

Vsako dobljeno vsoto ločimo po spremenljivkah s in r ter koerficiente zapišemo s pomočjo odvodov

$$\frac{1}{2} \left(\sum_{r,s=-\infty}^{\infty} (2r+1)^2 x^{r^2+r+s^2} - \sum_{r,s=-\infty}^{\infty} (2s)^2 x^{r^2+r+s^2} \right) =$$

$$= \frac{1}{2} \left(\sum_{s=-\infty}^{\infty} x^{s^2} \cdot \sum_{r=-\infty}^{\infty} (2r+1)^2 x^{r^2+r} - \sum_{r=-\infty}^{\infty} x^{r^2+r} \cdot \sum_{s=-\infty}^{\infty} (2s)^2 x^{s^2} \right) =$$

$$= \frac{1}{2} \left(\sum_{s=-\infty}^{\infty} x^{s^2} \cdot (1 + 4x\frac{d}{dx}) \sum_{r=-\infty}^{\infty} x^{r^2+r} - \sum_{r=-\infty}^{\infty} x^{r^2+r} \cdot 4x\frac{d}{dx} \sum_{s=-\infty}^{\infty} x^{s^2} \right). \qquad (6.14)$$

Vsako vsoto po s zamenjamo s produktom, ki ga dobimo, če v enačbo 2. vstavimo $z = 1$, ter vsako vsoto po r zamenjamo s produktom, ki ga dobimo, če v enačbo 2. vstavimo $z = x$. Oglejmo si najprej, kaj dobimo, če v enačbo 2. vstavimo $z = 1$:

$$\prod_{n=1}^{\infty} (1-x^{2n})(1+zx^{2n-1})(1+z^{-1}x^{2n-1}) = \sum_{n=-\infty}^{\infty} z^n x^{n^2},$$

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+1\cdot x^{2n-1})(1+1^{-1}x^{2n-1}) = \sum_{n=-\infty}^{\infty} 1^n x^{n^2},$$

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1})^2 = \sum_{n=-\infty}^{\infty} x^{n^2}. \tag{6.15}$$

Poglejmo še primer, ko v enačbo 2. vstavimo $z = x$:

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+zx^{2n-1})(1+z^{-1}x^{2n-1}) = \sum_{n=-\infty}^{\infty} z^n x^{n^2},$$

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+x\cdot x^{2n-1})(1+x^{-1}x^{2n-1}) = \sum_{n=-\infty}^{\infty} x^n x^{n^2},$$

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n})(1+x^{2n-2}) = \sum_{n=-\infty}^{\infty} x^{n^2+n},$$

$$2\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n})^2 = \sum_{n=-\infty}^{\infty} x^{n^2+n}. \tag{6.16}$$

Dobljeni enakosti (6.15) in (6.16) vstavimo v (6.14) in dobimo

$$\frac{1}{2}\Big(\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1})^2\cdot(1+4x\frac{d}{dx})2\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n})^2$$

$$-2\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n})^2\cdot 4x\frac{d}{dx}(\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1})^2\Big) =$$

$$=\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1})^2\cdot(1+4x\frac{d}{dx})\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n})^2$$

$$-\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n})^2\cdot 4x\frac{d}{dx}(\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1})^2.$$

V dobljeni izraz vpeljemo oznake $a_n = 1+x^{2n}$, $b_n = 1+x^{2n-1}$ in $c_n = 1-x^{2n}$, ter dobimo

$$\prod_{n=1}^{\infty} c_n b_n^2\cdot(1+4x\frac{d}{dx})\prod_{n=1}^{\infty} c_n a_n^2 - \prod_{n=1}^{\infty} c_n a_n^2\cdot 4x\frac{d}{dx}\prod_{n=1}^{\infty} c_n b_n^2.$$

Če v zgornjem izrazu izračunamo odvode neskončnih produktov po pravilu

$$\left(\prod_{n=1}^{\infty} f_n\right)' = \prod_{n=1}^{\infty} f_n\cdot\sum_{n=1}^{\infty}\frac{f_n'}{f_n},$$

potem dobimo

$$\prod_{n=1}^{\infty} c_n b_n^2\cdot\prod_{n=1}^{\infty} c_n a_n^2 + \prod_{n=1}^{\infty} c_n b_n^2\cdot 4x\frac{d}{dx}\prod_{n=1}^{\infty} c_n a_n^2 - \prod_{n=1}^{\infty} c_n a_n^2\cdot 4x\frac{d}{dx}\prod_{n=1}^{\infty} c_n b_n^2 =$$

$$= \prod_{n=1}^{\infty}(a_n b_n c_n)^2 + 4x\left(\prod_{n=1}^{\infty} c_n b_n^2 \cdot \prod_{n=1}^{\infty} c_n a_n^2 \sum_{n=1}^{\infty} \frac{c_n' a_n^2 + c_n \cdot 2a_n a_n'}{c_n a_n^2}\right.$$
$$\left. - \prod_{n=1}^{\infty} c_n a_n^2 \cdot \prod_{n=1}^{\infty} c_n b_n^2 \sum_{n=1}^{\infty} \frac{c_n' b_n^2 + c_n \cdot 2b_n b_n'}{c_n b_n^2}\right).$$

Vpeljemo oznako $Q_n = (a_n b_n c_n)^2$ ter nadaljujemo z izračunom.

$$\prod_{n=1}^{\infty} Q_n + 4x\left(\prod_{n=1}^{\infty} Q_n \sum_{n=1}^{\infty} \frac{c_n' a_n^2 + c_n \cdot 2a_n a_n'}{c_n a_n^2} - \prod_{n=1}^{\infty} Q_n \sum_{n=1}^{\infty} \frac{c_n' b_n^2 + c_n \cdot 2b_n b_n'}{c_n b_n^2}\right) =$$
$$= \prod_{n=1}^{\infty} Q_n \left(1 + 4x \sum_{n=1}^{\infty}\left(\frac{c_n' a_n^2 + c_n \cdot 2a_n a_n'}{c_n a_n^2} - \frac{c_n' b_n^2 + c_n \cdot 2b_n b_n'}{c_n b_n^2}\right)\right) =$$
$$= \prod_{n=1}^{\infty} Q_n \left(1 + 4x \sum_{n=1}^{\infty}\left(\frac{c_n'}{c_n} + \frac{2a_n'}{a_n} - \frac{c_n'}{c_n} - \frac{2b_n'}{b_n}\right)\right) =$$
$$= \prod_{n=1}^{\infty} Q_n \left(1 + 8x \sum_{n=1}^{\infty}\left(\frac{a_n'}{a_n} - \frac{b_n'}{b_n}\right)\right) =$$
$$= \prod_{n=1}^{\infty} Q_n \left(1 + 8x \sum_{n=1}^{\infty}\left(\frac{2nx^{2n-1}}{1+x^{2n}} - \frac{(2n-1)x^{2n-2}}{1+x^{2n-1}}\right)\right) =$$
$$= \prod_{n=1}^{\infty} Q_n \left(1 + 8 \sum_{n=1}^{\infty}\left(\frac{2nx^{2n}}{1+x^{2n}} - \frac{(2n-1)x^{2n-1}}{1+x^{2n-1}}\right)\right) =$$
$$= \prod_{n=1}^{\infty} Q_n \left(1 - 8 \sum_{n=1}^{\infty}\left(\frac{(2n-1)x^{2n-1}}{1+x^{2n-1}} - \frac{2nx^{2n}}{1+x^{2n}}\right)\right).$$

S tem smo dobili natanko enačbo 6.

7.: Enačbo 7. izpeljemo s pomočjo oznake Q_n.

$$Q_n = (a_n b_n c_n)^2 = (1+x^{2n})^2(1+x^{2n-1})^2(1-x^{2n})^2.$$

Vemo, da velja

$$1 - x^{2n} = (1-x^n)(1+x^n) \tag{6.17}$$

in

$$\prod_{n=1}^{\infty}(1+x^{2n})(1+x^{2n-1}) = (1+x^2)(1+x)(1+x^4)(1+x^3)\cdots = \prod_{n=1}^{\infty}(1+x^n). \tag{6.18}$$

Z upoštevanjem enačbe (6.17) in enačbe (6.18) izpeljemo

$$\prod_{n=1}^{\infty} Q_n = \prod_{n=1}^{\infty}(1+x^{2n})^2(1+x^{2n-1})^2(1-x^{2n})^2 =$$
$$= \prod_{n=1}^{\infty}(1+x^n)^2(1+x^n)^2(1-x^n)^2 = \prod_{n=1}^{\infty}(1+x^n)^4(1-x^n)^2.$$

S tem smo dokazali enačbo 7.

Primer 6.2. Oglejmo si naravno število 4. Njeni deljitelji so 1, 2 in 4. Torej po formuli velja, da lahko 4 zapišemo kot vsoto štirih kvadratov na

$$8((1+2+4)-(4)) = 8(7-4) = 8 \cdot 3 = 24$$

načinov.

$$\begin{aligned} 4 &= (\pm 2)^2 + 0^2 + 0^2 + 0^2 \\ &= 0^2 + (\pm 2)^2 + 0^2 + 0^2 \\ &= 0^2 + 0^2 + (\pm 2)^2 + 0^2 \\ &= 0^2 + 0^2 + 0^2 + (\pm 2)^2 \\ &= (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 \end{aligned}$$

■

Primer 6.3. Oglejmo si še naravno število 10. Njegovi deljitelji so 1, 2, 5 in 10. Torej ga lahko napišemo na

$$8((1+2+5+10)-(0)) = 8 \cdot 18 = 144$$

načinov kot vsoto štirih kvadratov.

$$\begin{aligned} 10 &= (\pm 3)^2 + (\pm 1)^2 + 0^2 + 0^2 \\ &= (\pm 3)^2 + 0^2 + (\pm 1)^2 + 0^2 \\ &= (\pm 3)^2 + 0^2 + 0^2 + (\pm 1)^2 \\ &= (\pm 1)^2 + (\pm 3)^2 + 0^2 + 0^2 \\ &= 0^2 + (\pm 3)^2 + (\pm 1)^2 + 0^2 \\ &= 0^2 + (\pm 3)^2 + 0^2 + (\pm 1)^2 \\ &= (\pm 1)^2 + 0^2 + (\pm 3)^2 + 0^2 \\ &= 0^2 + (\pm 1)^2 + (\pm 3)^2 + 0^2 \\ &= 0^2 + 0^2 + (\pm 3)^2 + (\pm 1)^2 \\ &= (\pm 1)^2 + 0^2 + 0^2 + (\pm 3)^2 \\ &= 0^2 + (\pm 1)^2 + 0^2 + (\pm 3)^2 \\ &= 0^2 + 0^2 + (\pm 1)^2 + (\pm 3)^2 \end{aligned} \qquad \begin{aligned} &= (\pm 2)^2 + (\pm 2)^2 + (\pm 1)^2 + (\pm 1)^2 \\ &= (\pm 2)^2 + (\pm 1)^2 + (\pm 2)^2 + (\pm 1)^2 \\ &= (\pm 2)^2 + (\pm 1)^2 + (\pm 1)^2 + (\pm 2)^2 \\ &= (\pm 1)^2 + (\pm 2)^2 + (\pm 2)^2 + (\pm 1)^2 \\ &= (\pm 1)^2 + (\pm 2)^2 + (\pm 1)^2 + (\pm 2)^2 \\ &= (\pm 1)^2 + (\pm 1)^2 + (\pm 2)^2 + (\pm 2)^2 \end{aligned}$$

■

7 ZAKLJUČEK

Vsako naravno število lahko predstavimo kot vsoto štirih kvadratov, pri čemer so nekateri lahko 0. Torej, brez ničelnih členov lahko nekatera števila zapišemo tudi kot vsoto samo dveh ali treh kvadratov.

Z vsakim odgovorom se pojavijo nova vprašanja. Katero je nejmanjše naravno število n, da lahko vsako naravno število zapišemo kot n kubov ali n členov na višje potence? Leta 1770 je Edward Waring v svojem delu Meditations Algebraicae dokazal, da lahko vsako število zapišemo kot vsoto devetih kubov ter da lahko vsako število zapišemo kot vsoto devetnajstih členov na četrto potenco. Na podlagi tega se je izoblikoval matematiče problem: Ali lahko vsako število zapišemo kot vsoto $g(k)$ celih števil na k-to potenco, kjer je $g(k)$ odvisen samo od k? Mi smo pokazali, da je $g(2) = 4$. Matematiku Helbertu je uspelo leta 1909 pokazati, da $g(k)$ obstaja za vsak k, vendar kako velik je $g(k)$ pa zaenkrat ostaja še vedno odprt problem.

Oglejmo si primer zapisa števila 239 kot vsoto devetih kubov

$$239 = 4^3 + 4^3 + 3^3 + 3^3 + 3^3 + 3^3 + 1^3 + 1^3 + 1^3.$$

To je tudi edino število, ki v svoji vsoti potrebuje devet kubov, vsa števila večja od njega potrebujejo samo osem ali manj kubov v svoji vsoti. Do sedaj jim je uspelo dokazati tudi, da lahko vsako število zapišemo kot vsoto 37 členov na peto potenco, ter da za števila manjša od 10^{310} ter večja od 10^{1409} velja, da je $g(4) = 19$.

Še zanimivejše vprašanje je, katera števila na n-to potenco lahko zapišemo kot vsoto n členov na n-to potenco. Leta 1911 je bilo najdeno najmanše število na četrto potenco, ki ga lahko zapišemo kot vsoto štirih členov na četrto potenco

$$35^4 = 30^4 + 120^4 + 272^4 + 315^4.$$

Kmalu zatem je bila najdena še najmanjša rešitev za peto potenco

$$72^5 = 19^5 + 43^5 + 46^5 + 47^5 + 67^5.$$

Problem lahko še bolj omejimo: ali obstaja število na n-to potenco, ki ga lahko zapišemo kot vsoto manj kot n členov na n-to potenco? Odgovor je da. Leta 1968 sta Lander in Parkin odkrila

$$144^5 = 27^5 + 84^5 + 110^5 + 133^5.$$

8 LITERATURA IN VIRI

[1] D. M. Burton, *Elementary number theory*, University of New Hampshire, Boston, 1980, 67-109, 133-217, 259-285. *(Citirano na straneh 1, 2, 3, 5, 8, 10, 11, 13, 14, 25, 27, 28, 29, 31, 32, 33, 34, 38, 39 in 45.)*

[2] M. Aigner in G. M. Ziegler, *Proofs from the book, Third Edition.* Springer, Berlin, 2003, 17-22, 139. *(Citirano na strani 28.)*

[3] E. Landau, P. T. Bateman in E. E. Kohlbecker, *Elementary number theorem.* New York, Chelsea, 1927, Second edition translated into English by Jacob E. Goodman, 1966. *(Citirano na straneh 2, 36, 37 in 40.)*

[4] D. R. Wilkins, Part I: Topics in Number Theory. V *Course 311: Michaelmas Term 1999*, 1999, 14-25. *(Citirano na straneh 5, 16, 18, 21 in 22.)*

[5] M. Klazar, Jacobi's four squares identity. V *lecture on the 7-th PhD conference*, 2013, 1-5. *(Citirano na straneh 51 in 54.)*

[6] T. Pham, Dirichlet's Theorem on Arithmetic Progressions. V *Massachusetts Institute of Technology*, 21. maj 2012, 1-11. *(Citirano na strani 40.)*